

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

[Présentation du DRAC 5](#)
[Installation et configuration du DRAC 5](#)
[Configuration et utilisation de la console de ligne de commande du DRAC 5](#)
[Configuration du DRAC 5 via l'interface utilisateur Web](#)
[Récupération et dépannage du système géré](#)
[Utilisation du DRAC 5 avec Microsoft Active Directory](#)
[Utilisation de la redirection de console d'interface utilisateur graphique](#)
[Utilisation et configuration du média virtuel](#)
[Utilisation de l'interface de ligne de commande RACADM](#)
[Déploiement de votre système d'exploitation via VM-CLI](#)
[Utilisation de l'interface de ligne de commande SM-CLP DRAC 5](#)
[Dépannage](#)
[Présentation de la sous-commande RACADM](#)
[Définitions des groupes et des objets de la base de données de propriétés du DRAC 5](#)
[Interfaces RACADM prises en charge](#)
[Pré-installation du navigateur](#)
[Glossaire](#)

Remarques et avis

-  **REMARQUE** : Une REMARQUE indique des informations importantes qui vous permettent de mieux utiliser votre ordinateur.
-  **AVIS** : Un AVIS vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.
-

Les informations contenues dans le présent document sont sujettes à modification sans préavis.
© 2007 Dell Inc. Tous droits réservés.

Toute reproduction, de quelque manière que ce soit, sans l'autorisation écrite de Dell Inc. est strictement interdite.

Marques utilisées dans ce texte : *Dell*, le logo *DELL*, *Dell OpenManage* et *PowerEdge* sont des marques de Dell Inc. ; *Microsoft*, *Active Directory*, *Internet Explorer*, *Windows*, *Windows NT* et *Windows Server* sont des marques déposées et *Windows Vista* est une marque de Microsoft Corporation ; *Red Hat* est une marque déposée de Red Hat, Inc. ; *Novell* et *SUSE* sont des marques déposées de Novell Corporation. *Intel* est une marque déposée de Intel Corporation ; *UNIX* est une marque déposée de The Open Group aux États-Unis d'Amérique et dans d'autres pays.

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

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

Janvier 2007 Rev. A00

[Retour à la page du sommaire](#)

Présentation de la sous-commande RACADM

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [help](#)
- [arp](#)
- [clearasrscreen](#)
- [config](#)
- [getconfig](#)
- [coredump](#)
- [coredumpdelete](#)
- [fwupdate](#)
- [getssninfo](#)
- [getsysinfo](#)
- [gettractime](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [setniccfq](#)
- [getniccfq](#)
- [getsvctag](#)
- [racdump](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [clrraclog](#)
- [getsel](#)
- [clrsel](#)
- [gettracelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)
- [vmkey](#)

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 **d'ouvrir une session DRAC 5**.

Le [tableau A-1](#) décrit la commande **help**.

Tableau A-1. Commande help

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

Synopsis

```
racadm help
```

```
racadm help <sous-commande>
```

Description

La sous-commande **help** répertorie toutes les sous-commandes disponibles sous 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 de **racadm help < sous-commande >** n'affiche des informations que pour la sous-commande spécifiée.

Interfaces prises en charge

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

arp

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

Le [tableau A-2](#) décrit la commande arp.

Tableau A-2. Commande arp

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

Synopsis

```
racadm arp
```

Interfaces prises en charge

- 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

cleararscreen

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

Le [tableau A-3](#) décrit la sous-commande cleararscreen.

Tableau A-3. cleararscreen

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

Synopsis

```
racadm cleararscreen
```

Interfaces prises en charge

- 1 RACADM locale

- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

config

 **REMARQUE :** Pour utiliser la commande `getconfig`, vous devez avoir le droit d'**ouvrir une session DRAC 5**.

Le [tableau A-4](#) décrit les sous-commandes `config` et `getconfig`.

Tableau A-4. `config/getconfig`

Sous-commande	Définition
<code>config</code>	Configure le DRAC 5.
<code>getconfig</code>	Récupère les données de configuration 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

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

Description

La sous-commande `config` permet à l'utilisateur de définir les paramètres de configuration DRAC 5 individuellement ou de les regrouper dans un fichier de configuration. Si les données sont différentes, l'objet DRAC 5 est récrit avec la nouvelle valeur.

Entrées

Le [tableau A-5](#) décrit les options de la sous-commande `config`.

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

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

Option	Description
<code>-f</code>	L'option <code>-f <nom de fichier></code> force <code>config</code> à lire le contenu du fichier <code><nom de fichier></code> et à configurer DRAC 5. Le fichier doit contenir des données dans le format spécifié par les « règles d'analyse ».
<code>-p</code>	L'option de mot de passe <code>-p</code> indique à <code>config</code> de supprimer les entrées de mots de passe contenues dans le fichier de configuration <code>-f <nom de fichier></code> une fois la configuration terminée.
<code>-g</code>	L'option de groupe, <code>-g <nom du groupe></code> , doit être utilisée avec l'option <code>-o</code> . Le <code><nom du groupe></code> spécifie le groupe contenant l'objet à définir.
<code>-o</code>	L'option d'objet, <code>-o <nom de l'objet> <Valeur></code> , doit être utilisée avec l'option <code>-g</code> . Cette option spécifie le nom d'objet écrit avec la chaîne <code><valeur></code> .
<code>-i</code>	L'option d'index, <code>-i <index></code> , n'est valable que pour les groupes indexés et peut être utilisée pour spécifier un groupe unique. L' <code><index></code> est un entier décimal compris entre 1 et 16. L'index est spécifié ici par la valeur de l'index, pas par une valeur « nommée ».
<code>-c</code>	L'option d'analyse <code>-c</code> est utilisée avec la sous-commande <code>config</code> et permet à l'utilisateur d'analyser le fichier <code>.cfg</code> afin de trouver les erreurs de syntaxe. Si des erreurs sont trouvées, le numéro de la ligne et une brève description de tout ce qui est inexact sont affichés. Il n'y a pas d'écritures sur 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 :

- 1 Syntaxe, nom du groupe, nom de l'objet, index non valide, ou d'autres éléments non valides de la base de données
- 1 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

```
1 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**.

```
1 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 entrées manuellement 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 commande getconfig

La sous-commande **getconfig** permet à l'utilisateur d'extraire les paramètres de configuration DRAC 5 un par un ou d'extraire et d'enregistrer dans un fichier l'ensemble des groupes de configuration RAC.

Entrées

Le [tableau A-6](#) décrit les options de la sous-commande **getconfig**.

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

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

Option	Description
-f	L'option -f <i><nom de fichier></i> 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 lots à l'aide de la sous-commande config . REMARQUE : L'option -f ne crée pas d'entrées pour les groupes cfgLpmiPet et cfgLpmiPef . Vous devez définir au moins une destination d'interruption pour capturer le groupe cfgLpmiPet sur le fichier.
-g	L'option de groupe , -g <i><nom du groupe></i> , permet d'afficher la configuration d'un groupe unique. Le nom du groupe est le nom du groupe utilisé dans les fichiers racadm.cfg . Si le groupe est indexé, l'option -i doit être utilisée.
-h	L'option d' aide , -h , affiche la liste de tous les groupes de configuration 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 <i><index></i> , n'est valable que pour les groupes indexés et peut être utilisée pour spécifier un groupe unique. L' <i><index></i> est un entier décimal compris entre 1 et 16. Si <i><index></i> 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, pas par une valeur nommée.
-o	L'option -o <i><nom d'objet></i> ou l'option d'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 <i><nom d'utilisateur></i> , permet d'afficher la configuration de l'utilisateur spécifié. L'option de <i><nom d'utilisateur></i> 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 :

- 1 Syntaxe, nom du groupe, nom de l'objet, index non valide, ou d'autres éléments non valides de la base de données
- 1 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

```
1 racadm getconfig -g cfgLanNetworking
```

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

```
1 racadm getconfig -f myrac.cfg
```

Enregistre tous les objets de configuration de groupe du RAC sur `myrac.cfg`.

```
1 racadm getconfig -h
```

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

```
1 racadm getconfig -u root
```

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

```
1 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 propriété.

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

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

coredump

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

Le [tableau A-7](#) décrit la sous-commande `coredump`.

Tableau A-7. `coredump`

Sous-commande	Définition
<code>coredump</code>	Affiche la dernière image 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 disponible, les informations `coredump` sont permanentes dans les cycles d'alimentation de RAC et restent disponibles jusqu'à ce qu'une des conditions suivantes se produise :

- 1 Les informations `coredump` sont effacées avec la sous-commande `coredumpdelete`.
- 1 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

- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

coredumpdelete

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit d'effacer les journaux ou d'exécuter les commandes de débogage.

Le [tableau A-8](#) décrit la sous-commande `coredumpdelete`.

Tableau A-8. `coredumpdelete`

Sous-commande	Définition
<code>coredumpdelete</code>	Supprime l'image mémoire stockée 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

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

fwupdate

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

 **REMARQUE :** Avant de commencer la mise à jour du micrologiciel, reportez-vous à « [Mise à jour du micrologiciel DRAC 5](#) » pour de plus amples informations.

Le [tableau A-9](#) décrit la sous-commande `fwupdate`.

Tableau A-9. `fwupdate`

Sous-commande	Définition
<code>fwupdate</code>	Met le micrologiciel DRAC 5 à jour.

Synopsis

```
racadm fwupdate -s
```

```
racadm fwupdate -g -u -a <Adresse_IP_du_serveur_FTP> -d <chemin>
```

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

Description

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

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

Interfaces prises en charge

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

Entrées

Le [tableau A-10](#) décrit les options de la sous-commande **fwupdate**.

 **REMARQUE :** L'option **-p** est uniquement prise en charge dans une interface RACADM locale et pas avec la console série/Telnet/SSH.

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

Option	Description
-u	L'option mise à jour effectue une somme de contrôle sur le fichier de mise à jour du micrologiciel et démarre le processus de mise à jour. 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 état renvoie l'état actuel du processus de mise à jour. Cette option est toujours utilisée seule.
-g	L'option obtenir 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 répertoire , -d , spécifie le répertoire où se trouve le fichier de mise à jour de micrologiciel, sur le serveur TFTP ou sur le serveur qui héberge le DRAC 5.
-p	L'option -p , ou placer , est utilisée pour mettre à jour le fichier de micrologiciel du système géré vers 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

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

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 le **racadm** local.

```
1 racadm fwupdate -s
```

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

```
1 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.

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

Dans cet exemple, l'interface 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 sur 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 **d'ouvrir une session DRAC 5**.

Le [tableau A-11](#) décrit la sous-commande `getssninfo`.

Tableau A-11. Sous-commande `getssninfo`

Sous-commande	Définition
<code>getssninfo</code>	Récupère les informations de session d'une ou de plusieurs sessions actives ou en attente dans le tableau 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 :

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

Interfaces prises en charge

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

Entrées

Le [tableau A-12](#) décrit les options de la sous-commande `getssninfo`.

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

Option	Description
<code>-A</code>	L'option <code>-A</code> élimine l'impression des en-têtes de données.
<code>-u</code>	Avec l'option <code>-u <nom d'utilisateur></code> , les résultats imprimés ne contiennent que les enregistrements de session concernant le nom d'utilisateur donné. Si un « * » 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

```
1 racadm getssninfo
```

Le [tableau A-13](#) fournit un exemple de résultat de la commande `racadm getssninfo`.

Tableau A-13. Exemple de résultat de la sous-commande `getssninfo`

Utilisateur	Adresse IP	Type	Consoles
-------------	------------	------	----------

root	192.168.0.10	Telnet	KVM virtuel
------	--------------	--------	-------------

```
l racadm getssninfo -A
"root" 143.166.174.19 "Telnet" "NONE"
l 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 **d'ouvrir une session DRAC 5**.

Le [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 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 surveillance.

Interfaces prises en charge

- l RACADM locale
- l RACADM distante
- l RACADM Telnet/SSH/série

Entrées

Le [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 DRAC 5.
-s	Affiche les informations sur le système.
-w	Affiche les informations sur la surveillance.
-A	Élimine l'impression d'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 surveillance.

Exemple de résultat

```
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

```
l 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"

l 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 d'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.

getractive

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit **d'ouvrir une session DRAC 5**.

Le [tableau A-16](#) décrit la sous-commande `getractive`.

Tableau A-16. `getractive`

Sous-commande	Définition
<code>getractive</code>	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 l'heure au format *aaaammjjhhmmss.mmmmmms*, qui est le même format renvoyé par la commande UNIX **date**.

Résultat

La sous-commande **getractime** affiche le résultat sur une ligne.

Exemple de résultat

```
racadm getractime
Thu Dec 8 20:15:26 2005
racadm getractime -d
20051208201542.000000
```

Interfaces prises en charge

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

ifconfig

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit d'**exécuter des commandes de diagnostic** ou de **configurer le DRAC 5**.

Le [tableau A-17](#) décrit la sous-commande **ifconfig**.

Tableau A-17. ifconfig

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

Synopsis

racadm ifconfig

netstat

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

Le [tableau A-18](#) décrit la sous-commande **netstat**.

Tableau A-18. netstat

--	--

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

Synopsis

```
racadm netstat
```

Interfaces prises en charge

- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

ping

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit d'**exécuter des commandes de diagnostic** ou de **configurer le DRAC 5**.

Le [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 les informations actuelles 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

- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

setniccfg

 **REMARQUE :** Pour utiliser la commande **setniccfg**, vous devez avoir le droit de **configurer le DRAC 5**.

Le [tableau A-20](#) décrit la sous-commande **setniccfg**.

Tableau A-20. setniccfg

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

 **REMARQUE :** Les termes NIC et port de gestion Ethernet sont interchangeables.

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.

- 1 L'option **-d** active le protocole DHCP pour le port de gestion Ethernet (la valeur par défaut est DHCP activé).
- 1 L'option **-s** active les paramètres d'adresse 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 tapés sous forme de chaînes séparées par des points.

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

- 1 L'option **-o** désactive le port de gestion Ethernet complètement. *<adresse IP>*, *<masque de réseau>*, et *<passerelle>* doivent être tapés sous forme de chaînes 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

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

getniccfg

 **REMARQUE :** Pour utiliser la commande **getniccfg**, vous devez avoir le droit d'**ouvrir une session DRAC 5**.

Le [tableau A-21](#) décrit les sous-commandes **setniccfg** et **getniccfg**.

Tableau A-21. setniccfg/getniccfg

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

Synopsis

```
racadm getniccfg
```

Description

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

Exemple de résultat

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

```
NIC Enabled      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway          = 192.168.0.1
```

Interfaces prises en charge

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

getsvctag

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit **d'ouvrir une session DRAC 5**.

Le [tableau A-22](#) décrit la sous-commande **getsvctag**.

Tableau A-22. getsvctag

Sous-commande	Définition
getsvctag	Affiche un numéro de service.

Synopsis

```
racadm getsvctag
```

Description

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

Exemple

Tapez **getsvctag** à l'invite de commande. Le résultat s'affiche de la façon suivante :

```
y76TP0G
```

La sous-commande renvoie 0 en cas de réussite et des valeurs autre que zéro en cas d'erreur.

Interfaces prises en charge

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

racdump

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit d'effectuer des opérations de **débogage**.

Le [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, ou des informations générales sur une carte DRAC 5.

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

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

Interfaces prises en charge

- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

racreset

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

Le [tableau A-24](#) décrit la sous-commande **racreset**.

Tableau A-24. racreset

Sous-commande	Définition
racreset	Réinitialise le DRAC 5.

 **AVIS :** 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.

 **AVIS :** Vous devez redémarrer votre système après avoir effectué une réinitialisation matérielle du DRAC 5 comme décrit dans le [tableau A-25](#).

Le [tableau A-25](#) décrit les options de la sous-commande **racreset**.

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

Option	Description
hard	Une réinitialisation <i>matérielle</i> 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 <i>logicielle</i> effectue une opération de redémarrage normale sur le RAC.

Exemples

1 racadm racreset

Démarre la séquence de redémarrage logicielle du DRAC 5.

1 racadm racreset hard

Démarre la séquence de redémarrage matérielle du DRAC 5.

Interfaces prises en charge

1 RACADM locale

1 RACADM distante

1 RACADM Telnet/SSH/série

racresetcfg

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

Le [tableau A-26](#) décrit la sous-commande **racresetcfg**.

Tableau A-26. **racresetcfg**

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

Synopsis

racadm racresetcfg

Interfaces prises en charge

1 RACADM locale

1 RACADM distante

1 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.

 **AVIS :** Cette commande supprime votre configuration RAC actuelle et réinitialise les paramètres d'usine par défaut de RAC et de la configuration série. Après la réinitialisation, le nom d'utilisateur et le mot de passe par défaut sont **root** et **calvin**, respectivement, et l'adresse IP est 192.168.0.120. Si vous émettez une commande **racresetcfg** à partir d'un client réseau (par exemple, un navigateur Web pris en charge, une interface RACADM Telnet/SSH ou 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 d'**exécuter des commandes de contrôle du serveur**.

Le [tableau A-27](#) décrit la sous-commande **serveraction**.

Tableau A-27. **serveraction**

Sous-commande	Définition
---------------	------------

serveraction	Exécute une réinitialisation ou une mise hors puis sous tension du système géré.
--------------	--

Synopsis

```
racadm serveraction <action>
```

Description

La sous-commande `serveraction` permet aux utilisateurs d'effectuer des opérations de gestion de l'alimentation sur le système hôte. Le [tableau A-28](#) décrit les options de contrôle de l'alimentation `serveraction`.

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

Chaîne	Définition
<action>	Spécifie l'action. Les options de la chaîne <action> sont : <ul style="list-style-type: none"> <code>powerdown</code> : met le système géré hors tension. <code>powerup</code> : met le système géré sous tension. <code>powercycle</code> : 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 éteindre puis redémarrer le système. <code>powerstatus</code> : affiche l'état actuel de l'alimentation du serveur (« Activé » ou « Désactivé ») <code>hardreset</code> : 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 distante
- | RACADM Telnet/SSH/série

getraclog

 **REMARQUE** : Pour utiliser cette commande, vous devez avoir le droit **d'ouvrir une session DRAC 5**.

Le [tableau A-29](#) décrit la commande `racadm getraclog`.

Tableau A-29. `getraclog`

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

Synopsis

```
racadm getraclog -i
```

```
racadm getraclog [-A] [-o] [-c décompte] [-s enregistrement-démarrage] [-m]
```

Description

La commande `getraclog -i` affiche le nombre d'entrées du journal DRAC 5.

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

- 1 **-A** : affiche le résultat sans en-tête ou nom.
- 1 **-c** : fournit le nombre maximum d'entrées à renvoyer.
- 1 **-m** : affiche un écran d'informations à la fois et invite l'utilisateur à continuer (semblable à la commande **more** de UNIX).
- 1 **-o** : affiche le résultat sur une seule ligne.
- 1 **-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 indique le numéro d'enregistrement, la date/l'heure, la source et la description. L'horodatage commence à minuit, le 1^{er} janvier et augmente jusqu'à ce que le système redémarre. Après le redémarrage du système, l'horodatage du système est utilisé.

Exemple de résultat

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

Interfaces prises en charge

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

clrraclog

 **REMARQUE** : Pour utiliser cette commande, vous devez avoir le droit d'**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 d'**ouvrir une session DRAC 5**.

Le [tableau A-30](#) décrit la commande **getsel**.

Tableau A-30. **getsel**

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

Synopsis

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-o] [-c décompte] [-s décompte] [-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 le résultat sans affichage d'en-tête ou de nom.

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

-o : affiche le résultat sur une seule ligne.

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

-E : place les 16 octets de SEL brut à la fin de chaque ligne de résultat 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** de UNIX).

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

Résultat

L'affichage du résultat par défaut indique le numéro d'enregistrement, la date et l'heure, 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

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

clrsel

 **REMARQUE** : Pour utiliser cette commande, vous devez avoir le droit d'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

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

gettracelog

 **REMARQUE :** Pour utiliser cette commande, vous devez avoir le droit **d'ouvrir une session DRAC 5**.

Le [tableau A-31](#) décrit la sous-commande **gettracelog**.

Tableau A-31. gettracelog

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

Synopsis

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c décompte] [-s enregistrement démarrage] [-m]
```

Description

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

- i : affiche le nombre d'entrées du journal de suivi du DRAC 5
- m : affiche un écran à la fois et invite l'utilisateur à continuer (semblable à la commande **more** de UNIX).
- o : affiche le résultat 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 du résultat par défaut indique le nombre d'enregistrements, la date et l'heure, la source et la description. L'horodatage commence à minuit, le 1^{er} janvier et augmente jusqu'à ce que le système redémarre. Après le redémarrage 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

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

sslcsrgen

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

Le [tableau A-32](#) décrit la sous-commande **sslcsrgen**.

Tableau A-32. sslcsrgen

--	--

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

Synopsis

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

```
racadm sslcsrgen -s
```

Description

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

Options

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

Le [tableau A-33](#) décrit les options de la sous-commande **sslcsrgen**.

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

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

 **REMARQUE :** Si l'option **-f** n'est pas spécifiée, le nom de fichier sera **sslcsr** par défaut et sera 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 :

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

Restrictions

La sous-commande **sslcsrgen** peut seulement être exécutée à partir d'un client RACADM local ou distant 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 RACADM [cfgRacSecurity](#). Par exemple :
racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MaCompagnie

Exemples

```
racadm sslcsrgen -s
```

ou

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

Interfaces prises en charge

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

sslcertupload

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

Le [tableau A-34](#) décrit la sous-commande **sslcertupload**.

Tableau A-34. sslcertupload

Sous-commande	Description
sslcertupload	Télécharge un serveur SSL personnalisé ou un certificat d'une autorité de certification à partir du client sur le RAC.

Synopsis

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

Options

Le [tableau A-35](#) décrit les options de la sous-commande **sslcertupload**.

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

Option	Description
-t	Spécifie le type de certificat à télécharger, soit le certificat de l'autorité de certification, soit le certificat du serveur. 1 = certificat du serveur 2 = certificat d'autorité de certification
-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 RACADM local ou distant. 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

- 1 RACADM locale
- 1 RACADM distante

sslcertdownload

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

Le [tableau A-36](#) décrit la sous-commande **sslcertdownload**.

Tableau A-36. sslcertdownload

Sous-commande	Description
---------------	-------------

<code>sslcertupload</code>	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

Le [tableau A-37](#) décrit les options de la sous-commande `sslcertdownload`.

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

Option	Description
<code>-t</code>	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
<code>-f</code>	Spécifie le nom de fichier du certificat à télécharger Si l'option <code>-f</code> ou le nom de fichier ne sont pas spécifiés, le fichier <code>sslcert</code> 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 RACADM local ou distant. 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

- 1 RACADM locale
- 1 RACADM distante

sslcertview

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

Le [tableau A-38](#) décrit la sous-commande `sslcertview`.

Tableau A-38. `sslcertview`

Sous-commande	Description
<code>sslcertview</code>	Affiche le serveur SSL ou le certificat d'une autorité de certification qui existe sur le RAC.

Synopsis

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

Options

Le [tableau A-39](#) décrit les options de la sous-commande `sslcertview`.

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

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

Exemple de résultat

```
racadm sslcertview -t 1
```

```
Serial Number          : 00

Subject Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)      : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : 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
DRAC5 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces prises en charge

- | RACADM locale
- | RACADM distante
- | RACADM Telnet/SSH/série

testemail

Le [tableau A-40](#) décrit la sous-commande `testemail`.

Tableau A-40. 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 RACADM [cfgEmailAlert](#) est activé et configuré correctement. Le [tableau A-41](#) fournit une liste et les commandes associées pour le groupe [cfgEmailAlert](#).

Tableau A-41. 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 utilisateur1@macompagnie.com
Définir le message personnalisé qui est envoyé à l'adresse e-mail de destination	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "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

Le [tableau A-42](#) décrit les options de la sous-commande testemail.

Tableau A-42. Sous-commandes testemail

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

Résultat

Aucun.

Interfaces prises en charge

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

testtrap

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

Le [tableau A-43](#) décrit la sous-commande testtrap.

Tableau A-43. 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 spécifié sur le réseau.

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

Le [tableau A-41](#) fournit une liste et les commandes associées pour le groupe [cfgIpmiPet](#).

Tableau A-44. 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

Entrées

Le [tableau A-45](#) décrit les options de la sous-commande **testtrap**.

Tableau A-45. 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

- 1 RACADM locale
- 1 RACADM distante
- 1 RACADM Telnet/SSH/série

vmdisconnect

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

Le [tableau A-46](#) décrit la sous-commande **vmdisconnect**.

Tableau A-46. 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 son état de manière appropriée. Cette sous-commande n'est disponible que si vous utilisez un utilitaire racadm local ou distant.

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 racadm [getsysinfo](#).

Interfaces prises en charge

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

vmkey

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

Le [tableau A-47](#) décrit la sous-commande **vmkey**.

Tableau A-47. 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 taille par défaut de la mémoire du disque flash virtuel est réinitialisée sur 16 Mo.

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 de la clé, qui est de 16 Mo sur le DRAC 5.

Interfaces prises en charge

- 1 RACADM locale
 - 1 RACADM distante
 - 1 RACADM Telnet/SSH/série
-

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

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

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Caractères affichables](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgRemoteHosts](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgNetTuning](#)
- [cfgOobSnmp](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgIpmiSerial](#)
- [cfgIpmiSol](#)
- [cfgIpmiLan](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)

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 de 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 chacun des objets 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 :

abcdefghijklmnopqrstuvwxyz

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 version du micrologiciel du RAC actuel. Par exemple, « 05.12.06 ».

Description

Chaîne de caractères contenant le numéro de version 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. Tous les 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 ; les utilisateurs devront se reconnecter en utilisant les nouveaux paramètres de l'adresse IP.

cfgDNSDomainNameFromDHCP (lecture/écriture)

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

Valeurs valides

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

 **REMARQUE** : Microsoft® Active Directory® ne prend en charge que les noms de domaine complets (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 de **configurer le DRAC 5**.

Valeurs valides

Chaîne de 63 caractères ASCII au maximum. Au moins un caractère doit être une lettre.

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

Valeur par défaut

rac-numéro de service

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 de **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 de **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 de **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 de **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 de **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 de **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 de **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 de 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 de **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 de **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 de **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 de réseau du RAC (NIC). Le [tableau B-1](#) décrit les modes pris en charge.

Tableau B-1. Modes pris en charge pour `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 de **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 de **configurer le DRAC 5**.

Valeurs valides

0 - 4094

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 de **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.

cfgRhostsSmtServerIpAddr (lecture/écriture)

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

Valeurs valides

Chaîne de caractères représentant une adresse IP de serveur SMTP valide. 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 de **configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

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

cfgRhostsFwUpdateIpAddr (lecture/écriture)

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

Valeurs valides

Chaîne de caractères représentant une adresse IP de serveur TFTP valide. 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 de micrologiciel du RAC via TFTP.

cfgRhostsFwUpdatePath (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 255.

Valeur par défaut

..

Description

Spécifie le chemin TFTP où le fichier image de micrologiciel du RAC existe sur le serveur TFTP. Le chemin TFTP est relatif au chemin 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 de 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 de **configurer des 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 de **configurer des 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 de configurer des utilisateurs.

Valeurs valides

de 0x0000000 à 0x00001ff et 0x0

Valeur par défaut

0x0000000

Description

Cette propriété spécifie les privilèges basés sur le rôle qui sont autorisés pour l'utilisateur. La valeur est représentée comme un masque binaire qui autorise n'importe quelle combinaison de valeurs de privilège. Le [tableau B-2](#) décrit les masques binaires des privilèges d'utilisateur autorisés.

Tableau B-2. Masques binaires des droits d'utilisateur

Droit d'utilisateur	Masque binaire de privilège
Ouverture d'une session DRAC 5	0x0000001
Configuration du DRAC 5	0x0000002
Configuration des utilisateurs	0x0000004
Effacement des journaux	0x0000008
Exécution des commandes de contrôle du serveur	0x0000010
Accès à la redirection de console	0x0000020
Accès au média virtuel	0x0000040
Test des alertes	0x0000080
Exécution des commandes de débogage	0x0000100

Exemples

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

Tableau B-3. Exemple de masques binaires pour les droits d'utilisateur

Droit(s) d'utilisateur	Masque binaire de privilège
L'utilisateur n'est pas autorisé à accéder au RAC.	0x0000000
L'utilisateur peut seulement se connecter au RAC et afficher les informations de configuration du RAC et du serveur.	0x0000001
L'utilisateur peut se connecter au RAC et modifier la configuration.	0x0000001 + 0x0000002 = 0x0000003
L'utilisateur peut se connecter au RAC, accéder au média virtuel et à la redirection de console.	0x0000001 + 0x0000040 + 0x0000080 = 0x00000C1

cfgUserAdminUserName (lecture/écriture)

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de configurer des utilisateurs.

Valeurs valides

Chaîne. Longueur maximale = 16.

Valeur par défaut

""

Description

Le nom d'utilisateur pour cet index. L'index utilisateur est créé en écrivant une chaîne 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 ne peut pas contenir de barre oblique « / », de barre oblique inverse « \ », de point « . », d'arobase « @ » ou de guillemets (").

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

cfgUserAdminPassword (lecture seule)

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de configurer des 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 la propriété écrite.

cfgUserAdminEnable

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de configurer des 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 de configurer des utilisateurs.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive un accès utilisateur SOL (Communications série sur le 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 des alertes e-mail. Par exemple, `utilisateur1@compagnie.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. 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 de **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 de **configurer le DRAC 5**.

Valeurs valides

10 - 1920

Valeur par défaut

30

Description

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

cfgSsnMgtWebserverTimeout (lecture/écriture)

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

Valeurs valides

60 - 1920

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 se ferme une fois la durée définie par cette propriété atteinte. Les modifications de ce paramètre n'affectent pas les sessions déjà ouvertes (vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte).

Une session de serveur Web expirée ferme la session actuelle.

cfgSsnMgtSshIdleTimeout (lecture/écriture)

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

Valeurs valides

0 (pas de délai d'attente)

60 - 1920

Valeur par défaut

300

Description

Définit la période d'inactivité attribuée à 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 se ferme une fois la durée définie par cette propriété atteinte. Les modifications de ce paramètre n'affectent pas les sessions déjà ouvertes (vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte).

Une session Secure Shell 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 de **configurer le DRAC 5**.

Valeurs valides

0 (pas de délai d'attente)

60 – 1920

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 se ferme une fois la durée définie par cette propriété atteinte. Les modifications de ce paramètre n'affectent pas les sessions déjà ouvertes (vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte).

Une session 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 de **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 de **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 de **configurer le DRAC 5**.

Valeurs valides

CHAÎNE

Longueur maximale = 4

Valeur par défaut

^\ (<Ctrl><\>)

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

Description

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

- 1 Valeur décimale - Par exemple : « 95 »
- 1 Valeur hexadécimale - Par exemple : « 0x12 »
- 1 Valeur octale - Par exemple : « 007 »
- 1 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 de **configurer le DRAC 5**.

Valeurs valides

0 = Pas de délai d'attente

60 – 1920

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 de **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 de **configurer le DRAC 5**.

Description

Spécifie une commande série qui est exécutée après qu'un utilisateur se connecte à l'interface de console série.

Valeur par défaut

""

Exemple

« connect com2 »

cfgSerialHistorySize (lecture/écriture)

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

Valeurs valides

0 – 8192

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 de **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 de **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 de **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.

 **AVIS** : Soyez 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 de **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. Si elle est activée, la négociation automatique a priorité sur les valeurs définies dans les objets `cfgNetTuningNic100MB` et `cfgNetTuningNicFullDuplex`.

cfgNetTuningNic100MB (lecture/écriture)

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

Valeurs valides

0 (10 Mo)

1 (100 Mo)

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 de **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 de **configurer le DRAC 5**.

Valeurs valides

576 – 1500

Valeur par défaut

1500

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 de **configurer le DRAC 5**.

Valeurs valides

6 – 384

Valeur par défaut

6

Description

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

cfgOobSnmpp

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.

cfgOobSnmppAgentCommunity (lecture/écriture)

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

Valeurs valides

Chaîne. 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 de **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 de RAC différentes, comme les ports valides et les restrictions de port de sécurité.

cfgRacTuneHttpPort (lecture/écriture)

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

Valeurs valides

10 – 65535

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 de **configurer le DRAC 5**.

Valeurs valides

10 – 65535

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 de **configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de validation de la plage d'adresse IP du RAC.

cfgRacTuneIpRangeAddr

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de **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 le profil 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 de **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.

cfgRacTuneIpBIkEnable

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

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgRacTuneIpBlkFailcount

 **REMARQUE :** Pour modifier cette propriété, vous devez avoir le droit de **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 de l'adresse IP soient rejetées.

cfgRacTuneIpBlkFailWindow

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

Valeurs valides

2 - 65535

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 de **configurer le DRAC 5**.

Valeurs valides

2 - 65535

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 de **configurer le DRAC 5**.

Valeurs valides

1 - 65535

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 de **configurer le DRAC 5**.

Valeurs valides

1 - 65535

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 de **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 de **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 de **configurer le DRAC 5**.

Valeurs valides

1 – 65535

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 nécessite une réinitialisation du DRAC 5 pour devenir actif.

cfgRacTuneConRedirVideoPort (lecture/écriture)

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

Valeurs valides

1 – 65535

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 nécessite une réinitialisation du DRAC 5 pour devenir actif.

cfgRacTuneAsrEnable (lecture/écriture)

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

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

 **REMARQUE** : Cet objet nécessite une réinitialisation du DRAC 5 pour devenir actif.

cfgRacTuneDaylightOffset (lecture/écriture)

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de **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 de **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 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 de **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 d'une interface RACADM distante. Cette propriété n'a aucun effet sur les interfaces RACADM Telnet/SSH/série ou locale.

cfgRacTuneLocalServerVideo (lecture/écriture)

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

Valeurs valides

1 (active)

0 (désactive)

Valeur par défaut

1

Description

Active (commutateur activé) ou désactive (commutateur désactivé) la vidéo du serveur local.

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 de **configurer le DRAC 5**.

Valeurs valides

Chaîne. 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 de **configurer le DRAC 5**.

Valeurs valides

Chaîne. 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 de 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.

cfgSecCsrCommonName (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le nom de domaine (CN) de la CSR.

cfgSecCsrOrganizationName (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

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

cfgSecCsrOrganizationUnit (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

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

cfgSecCsrLocalityName (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie la ville (L) de la CSR.

cfgSecCsrStateName (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le nom d'état (S) de la CSR.

cfgSecCsrCountryCode (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 2.

Valeur par défaut

""

Description

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

cfgSecCsrEmailAddr (lecture/écriture)

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

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie l'adresse e-mail de la CSR.

cfgSecCsrKeySize (lecture/écriture)

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

Valeurs valides

512

1024

2048

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 de 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 de **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 CDROM/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 d'**accéder au média virtuel**.

Valeurs valides

1 – 65535

Valeur par défaut

3669

Description

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

cfgVirAtapiSrvPortSsl (lecture/écriture)

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

Valeurs valides

Tout port disponible, en décimal, compris entre 0 et 65535.

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 de **configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgVirMediaBootOnce (lecture/écriture)

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

Valeurs valides

1 (activé)

0 (désactivé)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de démarrage unique de média virtuel du RAC. Si cette propriété est activée lorsque le serveur hôte est redémarré, cette fonctionnalité essaie de démarrer à partir des périphériques de média virtuel, si le média approprié est installé dans le périphérique.

cfgFloppyEmulation (lecture/écriture)

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

Valeurs valides

1 (True)

0 (False)

Valeur par défaut

1

Description

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

virtuel est reconnu comme un lecteur de disquette par les systèmes d'exploitation Windows. Les systèmes d'exploitation Windows lui attribuent la lettre de lecteur A: ou B:.

cfgActiveDirectory

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

cfgADRadDomain (lecture/écriture)

 **REMARQUE :** Pour modifier cette propriété, vous devez avoir le droit de **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.

cfgADRadName (lecture/écriture)

 **REMARQUE :** Pour modifier cette propriété, vous devez avoir le droit de **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 des DRAC enregistrés dans la forêt Active Directory.

cfgADEnable (lecture/écriture)

 **REMARQUE :** Pour modifier cette propriété, vous devez avoir le droit de **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.

cfgADAuthTimeout(lecture/écriture)

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de **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 de **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 du domaine.

cfgADType (lecture/écriture)

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de **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.

cfgStandardSchema

Ce groupe contient les paramètres qui permettent de configurer les paramètres du schéma standard.

cfgSSADRoleGroupIndex (lecture seule)

Valeurs valides

Entier de 1 à 5.

Description

Index du groupe de rôles enregistré dans Active Directory.

cfgSSADRoleGroupName (lecture/écriture)

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

Valeurs valides

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

Valeur par défaut

(aucune)

Description

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

cfgSSADRoleGroupDomain (lecture/écriture)

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

Valeurs valides

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

Valeur par défaut

(aucune)

Description

Domaine d'Active Directory où se trouve le groupe de rôles.

cfgSSADRoleGroupPrivilege (lecture/écriture)

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

Valeurs valides

De 0x00000000 à 0x000001ff

Valeur par défaut

(aucune)

Description

Utilisez les numéros des masques binaires du [tableau B-4](#) pour définir les privilèges d'autorité basés sur les rôles d'un groupe de rôles.

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

Privilège de groupes de rôles	Masque binaire
Ouverture d'une session DRAC 5	0x00000001
Configuration du DRAC 5	0x00000002
Configuration des utilisateurs	0x00000004
Effacement des journaux	0x00000008
Exécution des commandes de contrôle du serveur	0x00000010
Accès à la redirection de console	0x00000020
Accès au média virtuel	0x00000040
Test des alertes	0x00000080
Exécution des 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 de **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 avec 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 de **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 de **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 de **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 de **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 de **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 de **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 de **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 de **configurer le DRAC 5**.

Valeurs valides

- 0 (aucun)
- 1 (CR-LF)
- 2 (ZÉRO)
- 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 de **configurer le DRAC 5**.

Valeurs valides

- 0 (<ENTRÉE>)
- 1 (ZÉRO)

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 (communications série sur le LAN) du système.

cfgIpmiSolEnable (lecture/écriture)

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

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive les communications série sur le LAN (SOL).

cfgIpmiSolBaudRate (lecture/écriture)

 **REMARQUE :** Pour modifier cette propriété, vous devez avoir le droit de **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 de **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 l'accès aux communications série sur le LAN.

cfgIpmiSolAccumulateInterval (lecture/écriture)

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

Valeurs valides

1 à 255.

Valeur par défaut

10

Description

Spécifie le temps d'attente type du 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 de **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 le LAN du système.

cfgIpmiLanEnable (lecture/écriture)

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

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive l'interface IPMI sur le LAN.

cfgIpmiLanPrivLimit (lecture/écriture)

 **REMARQUE** : Pour modifier cette propriété, vous devez avoir le droit de **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 le LAN.

cfgIpmiLanAlertEnable (lecture/écriture)

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

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

cfgIpmiEncryptionKey (lecture/écriture)

 **REMARQUE** : Pour afficher ou modifier cette propriété, vous devez avoir le droit de **configurer le DRAC 5** et des droits d'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 de **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 plateforme 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. Longueur maximale = 255.

Valeur par défaut

Nom du filtre d'index.

Description

Spécifie le nom du filtre d'événements sur plateforme.

cfgIpmiPefIndex (lecture seule)

Valeurs valides

1 - 17

Valeur par défaut

Valeur d'index d'un objet de filtre d'événements sur plateforme.

Description

Spécifie l'index d'un filtre d'événements sur plateforme spécifique.

cfgIpmiPefAction (lecture/écriture)

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

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive un filtre d'événements sur plateforme spécifique.

cfgIpmiPet

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

cfgIpmiPetIndex (lecture/écriture)

 **REMARQUE :** Pour modifier cette propriété, vous devez avoir le droit de **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 de **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 de **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 du sommaire](#)

[Retour à la page du sommaire](#)

Interfaces RACADM prises en charge

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

Le tableau suivant fournit un aperçu des sous-commandes RACADM et de 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 distante
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	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓

✓ = Pris en charge ; ✗ = Non pris en charge

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Préinstallation du navigateur

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Obtention du progiciel d'installation du plug-in](#)
- [Installation du plug-in](#)

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.

AVIS : Dans un environnement client en lecture seule, si le micrologiciel DRAC 5 est mis à jour avec une version plus récente du plug-in, le plug-in VM installé n'est alors plus opérationnel. 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-là, il sera demandé au client d'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.

Obtention du progiciel d'installation du plug-in

Pour obtenir le progiciel d'installation du plug-in, procédez comme suit :

1. Ouvrez une session DRAC5 existante.
 2. Dans la barre d'adresses du navigateur, remplacez l'URL :

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


par :

```
https://<RAC_IP>/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 sous...**
 4. Sélectionnez un emplacement pour enregistrer le progiciel d'installation du plug-in.
-

Installation du plug-in

Pour installer le progiciel d'installation du plug-in, procédez comme suit :

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. Entrez le chemin 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 DRAC 5 cible ne contient pas une version plus récente du plug-in.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Présentation du DRAC 5

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Nouveautés de cette version DRAC 5](#)
- [Caractéristiques matérielles du DRAC 5](#)
- [Spécifications matérielles](#)
- [Connexions d'accès à distance prises en charge](#)
- [Fonctionnalités de sécurisation du DRAC 5](#)
- [Plates-formes prises en charge](#)
- [Systèmes d'exploitation pris en charge](#)
- [Navigateurs Web pris en charge](#)
- [Fonctionnalités](#)
- [Autres documents utiles](#)

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, la récupération de systèmes en panne et des fonctions de contrôle de l'alimentation pour les systèmes Dell PowerEdge™.

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 panne le plus récent (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 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 commencer, consultez la section « [Installation et configuration du DRAC 5](#) ».

Nouveautés de cette version DRAC 5

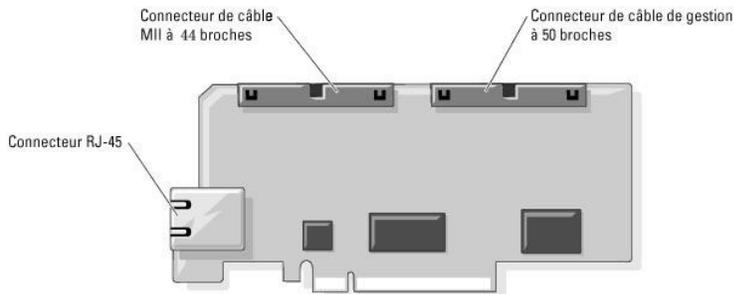
Pour cette version, la version 1.20 du micrologiciel DRAC 5 prend en charge les éléments suivants :

- 1 Schéma standard avec Microsoft Active Directory® : fournit des objets Active Directory standards à utiliser pour la gestion des utilisateurs et des privilèges d'utilisateur DRAC 5. Voir « [Présentation du schéma standard d'Active Directory](#) ».
- 1 Prise en charge d'une forêt et de plusieurs arborescences pour Active Directory : permet de prendre en charge l'authentification utilisateur sur plusieurs arborescences d'une même forêt sous Microsoft Active Directory. Voir « [Utilisation du DRAC 5 avec Active Directory : Questions les plus fréquentes](#) ».
- 1 Désactivation de la vidéo locale : donne la capacité d'activer et de désactiver la sortie vidéo du moniteur local d'un serveur, ce qui est utile pour la gestion de systèmes distants. Voir « [Désactivation ou activation de la vidéo locale](#) ».
- 1 Attribution d'une lettre de lecteur dans le média virtuel : donne une nouvelle fonctionnalité aux lecteurs de disquette virtuels. Un lecteur de disquette virtuel est reconnu comme une lettre de lecteur A: ou B: par les systèmes d'exploitation Windows et est énuméré comme un lecteur de disquette plutôt que comme un lecteur de disque amovible qui prend la lettre de lecteur C: ou une lettre plus élevée. Voir « [cfgFloppyEmulation \(lecture/écriture\)](#) ».

Caractéristiques matérielles du DRAC 5

La [figure 1-1](#) illustre le matériel du DRAC 5.

Figure 1-1. Caractéristiques matérielles du DRAC 5



Spécifications matérielles

Alimentation

Le [tableau 1-1](#) répertorie les spécifications électriques du DRAC 5.

Tableau 1-1. 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 +5V 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. Consultez la [figure 1-1](#) pour les connecteurs de câble 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 dédié**.

À l'aide des câbles de gestion et MII, vous pouvez configurer votre DRAC en trois modes séparés, selon vos besoins. Consultez la section « [Modes du DRAC](#) » dans « [Utilisation de l'interface de ligne de commande RACADM](#) » pour plus d'informations.

Ports du DRAC 5

Le [tableau 1-2](#) identifie les ports d'écoute utilisés par le DRAC 5 pour une connexion serveur. Le [tableau 1-3](#) identifie les ports que le DRAC 5 utilise comme client. Ces informations sont nécessaires pour ouvrir des firewalls pour pouvoir accéder à distance à un DRAC 5.

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

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

Tableau 1-3. Ports clients du DRAC 5

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

Connexions d'accès à distance prises en charge

Le [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	<ul style="list-style-type: none">1 Ethernet à 10/100 Mb/s1 Prise en charge de DHCP1 Interruptions SNMP et notifications d'événements par e-mail1 Interface réseau dédiée pour l'interface Web du DRAC 51 Prise en charge de la console Telnet/SSH et des commandes CLI RACADM, y compris les commandes de démarrage du système, de réinitialisation, de mise sous tension et d'arrêt
Port série	<ul style="list-style-type: none">1 Prise en charge de la console série et des commandes CLI racadm, y compris les commandes de démarrage du système, de réinitialisation, de mise sous tension et d'arrêt1 Prise en charge de la redirection de console texte vers un terminal ou un émulateur de terminal VT-100

Fonctionnalités de sécurisation du DRAC 5

Le DRAC 5 dispose des fonctionnalités de sécurité suivantes :

- 1 Authentification des utilisateurs via Microsoft Active Directory (en option) ou via les ID d'utilisateur et les mots de passe stockés sur le matériel
- 1 Autorité basée sur le rôle, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- 1 Configuration d'ID d'utilisateur et de mot de passe par l'interface Web ou la CLI RACADM
- 1 CLI RACADM et interface Web prenant 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.

- 1 Configuration du délai d'expiration de la session (en secondes) avec l'interface Web ou la CLI RACADM
- 1 Ports IP configurables (si applicable)
- 1 Secure Shell (SSH) qui utilise une couche de transport cryptée pour une sécurité plus élevée.
- 1 Nombre maximum d'échecs d'ouverture de session par adresse IP, avec blocage de l'ouverture de session à partir de l'adresse IP lorsque la limite est dépassée.
- 1 Plage d'adresses IP limitée pour les clients se connectant au DRAC 5

Plateformes prises en charge

Le DRAC 5 prend en charge les systèmes PowerEdge suivants :

- 1 1900
- 1 1950
- 1 2900
- 1 2950
- 1 2970
- 1 6950

Consultez le *Guide de compatibilité de Dell PowerEdge* situé sur le site Web de support Dell à l'adresse support.dell.com pour les dernières plateformes prises en charge.

Systèmes d'exploitation pris en charge

Le [tableau 1-5](#) énumère les systèmes d'exploitation qui prennent en charge le DRAC 5.

Consultez le *Guide de compatibilité de Dell OpenManage™ Server Administrator* situé sur le site Web de support Dell à l'adresse support.dell.com pour des informations récentes.

Tableau 1-5. Systèmes d'exploitation pris en charge

Gamme de systèmes d'exploitation	Système d'exploitation
Microsoft Windows	Windows 2000 Advanced Server avec Service Pack 4 (SP4).

	<p>Windows 2000 Server avec SP4.</p> <p>Windows Server 2003 R2, éditions Standard et Enterprise avec SP2 (32 bits)</p> <p>Windows Server 2003, édition Web avec SP2 (32 bits)</p> <p>Windows Server 2003 R2, éditions Standard et Enterprise avec SP2 (x86_64).</p> <p>Windows Server 2003 éditions X64 Standard et Enterprise avec SP1 et SP2.</p> <p>Windows Storage Server 2003 R2 éditions X64 Workgroup, Standard et Enterprise (x86_64).</p> <p>Windows Unified Data Storage Server 2003 éditions X64 Gold Standard et Enterprise X64 (x86_64).</p> <p>Windows Vista™.</p> <p>REMARQUE : Quand vous installez Windows Server 2003 avec Service Pack 1, tenez compte des modifications apportées aux paramètres de sécurité DCOM. Pour plus d'informations, consultez l'article 903220 sur le site Web de support de Microsoft à l'adresse support.microsoft.com/kb/903220.</p>
Red Hat® Linux	<p>Enterprise Linux WS, ES et AS, version 3 (x86 et x86_64).</p> <p>Enterprise Linux WS, ES et AS, version 4 (ia32 et x86_64).</p> <p>Enterprise Linux WS, ES et AS, version 4 (x86 et x86_64).</p> <p>Enterprise Linux 5 (x86 et x86-64).</p> <p>REMARQUE : Quand vous utilisez le DRAC 5 avec les systèmes Red Hat Enterprise Linux (version 5), la prise en charge est limitée à un nœud géré et à l'interface CLI racadm ; la console gérée (interface Web) n'est pas prise en charge.</p>
SUSE® Linux	<p>Enterprise Server 9 avec mises à jour 2 et 3 (x86_64).</p> <p>Enterprise Server 10 (Gold) (x86_64).</p>

Navigateurs Web pris en charge

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

Le [tableau 1-6](#) énumère les navigateurs Web qui prennent en charge le DRAC 5.

Consultez le *Guide de compatibilité de Dell OpenManage Server Administrator* situé sur le site Web de support Dell à l'adresse support.dell.com pour des informations récentes.

Tableau 1-6. Navigateurs Web pris en charge

Système d'exploitation	Navigateur Web pris en charge
Windows	<p>Internet Explorer 6.0 (32 bits) avec Service Pack 2 (SP2) uniquement pour Windows XP et Windows 2003 R2 SP2.</p> <p>Internet Explorer 7.0 uniquement pour Windows Vista, Windows XP et Windows 2003 R2 SP2.</p> <p>Pour afficher les versions localisées de l'interface Web du DRAC 5 :</p> <ol style="list-style-type: none"> Ouvrez Panneau de configuration sous Windows. Double-cliquez sur l'icône Options régionales et linguistiques. Sélectionnez l'emplacement de votre choix dans le menu déroulant de Options régionales (emplacement). <p>AVIS : Si vous exécutez le client de média virtuel, vous devez utiliser Internet Explorer 6.0 avec Service Pack 1 ou version ultérieure.</p>
Linux	<p>Mozilla Firefox 1.5 (32 bits) uniquement sur SUSE Linux (version 10).</p> <p>Mozilla Firefox 2.0 (32 bits).</p>

Désactivation de la fonctionnalité de liste blanche dans Mozilla Firefox

Firefox inclut une fonctionnalité « liste blanche » qui fournit une sécurité supplémentaire. Lorsque la fonctionnalité de liste blanche est activée, le navigateur exige les droits d'utilisateur nécessaires pour installer les plug-ins pour chaque site distinct qui accueille le plug-in. Ce processus vous impose d'installer un plug-in pour chaque nom IP/DNS de RAC distinct, bien que les versions de plug-in soient identiques.

Pour désactiver la fonctionnalité de liste blanche et éviter toute installation de plug-in répétitive et inutile, procédez comme suit :

1. Ouvrez une fenêtre de navigateur Web Firefox.
2. Dans le champ Adresse, tapez l'élément suivant et appuyez sur <Entrée> :

about:config

3. Dans la colonne **Nom de l'option**, recherchez et double-cliquez sur **xpinstall.whitelist.required**.

Les valeurs de **Nom de l'option**, **Statut**, **Type** et **Valeur** deviennent en gras. La valeur de **Statut** devient **défini par l'utilisateur** et celle de **Valeur** devient **false**.

4. Dans la colonne **Nom de l'option**, recherchez **xpinstall.enabled**.

Assurez-vous que **Valeur** est défini sur **true**. Sinon, double-cliquez sur **xpinstall.enabled** pour définir **Valeur** sur **true**.

Fonctionnalités

Le DRAC 5 dispose des fonctionnalités suivantes :

- 1 Enregistrement de système de noms de domaine dynamique (DNS)
 - 1 Gestion et surveillance du système à distance via une interface Web, une connexion série, un utilitaire RACADM distant ou une connexion Telnet.
 - 1 Prise en charge de l'authentification Active Directory : centralise tous les ID d'utilisateur et mots de passe DRAC 5 dans Active Directory à l'aide des schémas standard et étendu.
 - 1 Redirection de console : fournit les fonctions de clavier, vidéo et souris à distance.
 - 1 Média virtuel : permet à un système géré d'accéder à un lecteur de média sur la station de gestion.
 - 1 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.
 - 1 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.
 - 1 Alerte du RAC : signale les problèmes de nœud géré potentiels via des messages par e-mail ou une interruption SNMP à l'aide des paramètres **Dédié**, **Partagé avec basculement** ou **Partagé**.
 - 1 Configuration locale et distante : permet une configuration locale et distante à l'aide de l'utilitaire de ligne de commande RACADM.
 - 1 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.
 - 1 Prise en charge d'IPMI.
 - 1 Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système à distance via l'interface Web.
 - 1 Gestion de la sécurité de niveau mot de passe : empêche tout accès non autorisé à un système distant.
 - 1 Autorisation basée sur le rôle permettant 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 :

- 1 L'aide en ligne du DRAC 5 donne des informations sur l'utilisation de l'interface Web.
- 1 Le *Guide d'utilisation de Dell OpenManage™ IT Assistant* et le *Guide de référence de Dell OpenManage IT Assistant* donnent des informations sur IT Assistant.
- 1 Le *Guide d'utilisation de Dell OpenManage Server Administrator* donne des informations sur l'installation et l'utilisation de Server Administrator.
- 1 Le *Guide d'utilisation des 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.
- 1 Le *Guide d'utilisation des progiciels Dell Update Packages* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Packages dans le cadre de votre stratégie de mise à jour du système.

En outre, la documentation système suivante fournit des informations supplémentaires sur le système sur lequel le DRAC 5 est installé :

- 1 Le *Guide d'informations sur les produits* fournit des consignes de sécurité et des informations réglementaires importantes. Les informations sur la garantie sont incluses dans ce document ou sont fournies séparément.
- 1 Le *Guide d'installation en rack* et les *Instructions d'installation en rack* fournis avec votre rack décrivent comment installer votre système dans un rack.
- 1 Le *Guide de démarrage rapide* présente les fonctionnalités du système, la configuration du système et les spécifications techniques.
- 1 Le *Manuel du propriétaire du matériel* fournit des informations sur les fonctionnalités du système et décrit comment dépanner le système et installer ou remplacer des composants système.
- 1 La documentation du logiciel de gestion de systèmes décrit les fonctionnalités, les spécifications, l'installation et l'utilisation de base du logiciel.

- 1 La documentation du système d'exploitation décrit comment installer (au besoin), configurer et utiliser le logiciel du système d'exploitation.
- 1 La documentation des composants que vous avez achetés à part fournit des informations pour configurer et installer ces options.
- 1 Des mises à jour sont parfois incluses avec le système pour décrire les changements apportés au système, au logiciel ou à la documentation.

 **REMARQUE** : Lisez toujours ces mises à jour en premier car elles remplacent souvent les informations des autres documents.

- 1 Des notes de diffusion ou des fichiers lisez-moi sont parfois inclus pour décrire les toutes dernières mises à jour du système ou de la documentation, ou des références techniques complexes destinées aux utilisateurs confirmés ou aux techniciens.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Déploiement de votre système d'exploitation via VM-CLI

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Avant de commencer](#)
- [Création d'un fichier image de démarrage](#)
- [Préparation au déploiement](#)
- [Déploiement du système d'exploitation](#)

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

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

Dell Custom Factory Integration

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.

Exigences du réseau

Un partage réseau doit comprendre les composants suivants :

- 1 Fichiers de système d'exploitation
- 1 Pilotes obligatoires
- 1 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 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> of=<fichier de sortie>
```

Par exemple :

```
dd if=/dev/fd0 of=myfloppy.img
```

Création d'un fichier image pour 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 et 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 et préconfiguré, créez le fichier. Incluez les programmes et/ou 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, procédez comme suit :

 - 1 Suivez les procédures d'installation réseau standard
 - 1 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 :
 - 1 Intégrez 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 référence lors de l'intégration des utilitaires DRAC 5 dans votre application de déploiement de système d'exploitation existante.
 - 1 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 sur vos systèmes distants.

Avant de commencer, vérifiez l'exemple 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 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 :
 - o Adresse IP ou nom DDNS du DRAC 5
 - o Nom de fichier image de déploiement de démarrage
 - o Nom d'utilisateur DRAC 5
 - o Mot de passe utilisateur DRAC 5
 - b. À l'aide de RACADM, configurez l'option d'un **seul démarrage** du DRAC 5 cible.
 - c. À l'aide de RACADM, redémarrez le système DRAC 5.
-

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

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

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Prise en charge de SM-CLP DRAC 5](#)
- [Fonctionnalités de SM-CLP](#)

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 suivante : www.dmtf.org.

SM-CLP DRAC 5 est un protocole régi par DMTF et SMWG pour fournir des standards aux implémentations CLI de gestion de systèmes. De nombreux efforts ont été faits par une architecture SMASH définie qui doit servir de base à un ensemble de composants de gestion de systèmes plus standardisé. SMWG SM-CLP est un sous-composant de l'ensemble des efforts SMASH effectués par DMTF.

Prise en charge de SM-CLP DRAC 5

DRAC 5 est le premier produit RAC qui fournit la prise en charge du protocole de ligne de commande basé sur SM-CLP. L'interface SM-CLP est hébergée par le micrologiciel du contrôleur DRAC 5 et prend en charge les interfaces Telnet, SSH et série. L'interface SM-CLP 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 SM-CLP

La spécification SM-CLP fournit un ensemble commun de verbes SM-CLP standard qui peuvent être utilisés pour la gestion de systèmes simple via la CLI.

Le [tableau 11-1](#) fournit une liste de verbes CLI pris en charge.

Tableau 11-1. Verbes CLI pris en charge

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 cibles, les verbes et les sous-cibles.
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.

Opérations de gestion et cibles SM-CLP

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 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 le [tableau 11-1](#).

Opérations de gestion

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

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

Cibles

Le [tableau 11-2](#) fournit une liste des cibles fournies par SM-CLP pour prendre en charge ces opérations.

Tableau 11-2. 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.

Options

Le [tableau 11-3](#) énumère les options SM-CLP prises en charge.

Tableau 11-3. 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.

Format de sortie SM-CLP

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

Exemples de SM-CLP DRAC 5

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

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

Gestion de l'alimentation du serveur

Le [tableau 11-4](#) fournit des exemples d'utilisation de SM-CLP pour effectuer des opérations de gestion de l'alimentation sur un système géré.

Tableau 11-4. Opérations de gestion de l'alimentation du serveur

Opération	Syntaxe
Connexion au 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 DRAC5 SM-CLP System Management Shell, version 1.0 Copyright (c) 2004-2006 Dell, Inc. All Rights Reserved ->
Mise hors tension du serveur	- ->stop /system1 system1 has been stopped successfully
Mise sous tension du serveur à partir de l'état désactivé	- ->start /system1

	system1 has been started successfully
Redémarrage du serveur	->reset /system1 system1 has been reset successfully

Gestion SEL

Le [tableau 11-5](#) fournit des exemples d'utilisation de SM-CLP pour effectuer des opérations SEL sur le système géré.

Tableau 11-5. Opérations de gestion SEL

Opération	Syntaxe
Affichage du journal SEL	<pre>->show /system1/logs1/log1 /system1/logs1/log1</pre> <p>Targets: Record1 Record2 Record3 Record4 Record5</p> <p>Properties: InstanceID = IPMI:BMCL SEL Log MaxNumberOfRecords = 512 CurrentNumberOfRecords = 5 Name = IPMI SEL EnabledState = 2 OperationalState = 2 HealthState = 2 Caption = IPMI SEL Description = IPMI SEL ElementName = IPMI SEL</p> <p>Commands: cd show help exit version</p>
Affichage de l'enregistrement SEL	<pre>->show /system1/logs1/log1/record4 /system1/logs1/log1/record4</pre> <p>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</p> <p>Commands: cd show help exit version</p>
Effacement du journal SEL	<pre>->delete /system1/logs1/log1/record* All records deleted successfully</pre>

Navigation de la cible MAP

Le [tableau 11-6](#) 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 11-6. Opérations de navigation de cible MAP

Opération	Syntaxe
Naviguer vers la cible système et redémarrer	<pre>->cd system1 ->reset</pre> <p>REMARQUE : La cible par défaut actuelle est /.</p>
Naviguer vers la cible SEL et afficher les enregistrements du journal	<pre>->cd system1 ->cd logs1/log1</pre>

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

Propriétés du système

Le [tableau 11-7](#) énumère les propriétés du système qui sont affichées lorsque l'utilisateur tape ce qui suit :

```
show /system1
```

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

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

Tableau 11-7. Propriétés du système

Objet	Propriété	Description
CIM_ComputerSystem	Name	Identifiant unique d'une instance de système qui existe dans l'environnement d'entreprise. Longueur maximale = 256
	ElementName	Nom d'utilisateur convivial du système. Longueur maximale = 64
	NameFormat	Identifie la méthode de génération de noms. Valeurs : Autres, IP, Numérotation, HID, NWA, HWA, X25, ISDN, IPX, DCC, ICD, E.164, SNA, OID/OSI, WWN, NAA
	Dedicated	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=Firewall 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

		<p>21=Virtualisateur de stockage</p> <p>22=Bibliothèque de médias</p> <p>23=Nœud d'extension</p> <p>24=En-tête NAS</p> <p>25=NAS autocontenu</p> <p>26=Onduleur</p> <p>27=Téléphone IP</p> <p>28=Contrôleur de gestion</p> <p>29=Gestionnaire de châssis</p>
	ResetCapability	<p>Définit les méthodes de réinitialisation disponibles sur le système</p> <p>Valeurs :</p> <p>1=Autre</p> <p>2=Inconnu</p> <p>3=Désactivé</p> <p>4=Activé</p> <p>5=Non implémenté</p>
	CreationClassName	Superclasse d'où est extraite cette instance.
	EnabledState	<p>Indique les états activé/désactivé du système.</p> <p>Valeurs :</p> <p>0=Inconnu</p> <p>1=Autre</p> <p>2=Activé</p> <p>3=Désactivé</p> <p>4=Arrêter</p> <p>5=Inapplicable</p> <p>6=Activé mais hors ligne</p> <p>7=En cours de test</p> <p>8=Déferé</p> <p>9 = Acquiescement</p> <p>10=Démarrage</p>
	EnabledDefault	<p>Indique la configuration de démarrage par défaut pour l'état activé du système. Par défaut, le système est « Activé » (valeur = 2).</p> <p>Valeurs :</p> <p>2=Activé</p> <p>3=Désactivé</p> <p>4=Inapplicable</p> <p>5=Activé mais hors ligne</p> <p>6=Aucune valeur par défaut</p>
	RequestedState	<p>Indique le dernier état demandé ou souhaité pour le système.</p> <p>Valeurs :</p> <p>2=Activé</p> <p>3=Désactivé</p> <p>4=Arrêter</p> <p>5=Pas de changement</p>

		6=Hors ligne 7=Test 8=Déferé 9 =Acquiescement 10=Redémarrer 11=Réinitialiser 12=Inapplicable
	HealthState	Indique l'intégrité actuelle du système. Valeurs : 0=Inconnu 5=OK 10=Dégradé/Avertissement 15=Panne mineure 20=Panne majeure 30=Panne critique 35=Erreur irrécupérable
	OperationalStatus	Indique la condition actuelle du système. Valeurs : 0=Inconnu 1=Autre 2=OK 3=Dégradé 4=Stressé 5=Panne 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.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Dépannage

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

● [Dépannage du DRAC 5](#)

Dépannage du DRAC 5

Consultez les tableaux suivants pour faciliter le dépannage du DRAC 5 et de RACADM :

[Tableau 6-9](#), « [Utilisation du DRAC 5 avec Active Directory : Questions les plus fréquentes](#) »

[Tableau 7-7](#), « [Utilisation de la redirection de console : Questions les plus fréquentes](#) »

[Tableau 8-2](#), « [Utilisation du média virtuel : Questions les plus fréquentes](#) »

[Tableau 9-4](#), « [Utilisation des commandes série et racadm : Questions les plus fréquentes](#) »

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Installation et configuration du DRAC 5

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Avant de commencer](#)
- [Installation du matériel du DRAC 5](#)
- [Configuration de votre système pour utiliser un DRAC 5](#)
- [Présentation générale de l'installation du logiciel et de la configuration](#)
- [Installation du logiciel sur le système géré](#)
- [Installation du logiciel sur la station de gestion](#)
- [Configuration d'un navigateur Web pris en charge](#)
- [Configuration des propriétés du DRAC 5](#)
- [Configuration des paramètres réseau du DRAC 5](#)
- [Ajout et configuration des utilisateurs DRAC 5](#)
- [Mise à jour du micrologiciel DRAC 5](#)
- [Accès au DRAC 5 via un réseau](#)
- [Configuration d'IPMI](#)
- [Configuration des événements sur plateforme](#)

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 :

- 1 Matériel du DRAC 5 (déjà installé ou en kit séparé)
- 1 Procédures d'installation du DRAC 5 (situées dans ce chapitre)
- 1 CD *Dell PowerEdge Installation and Server Management*
- 1 CD *Dell Systems Management Consoles*
- 1 CD *Dell PowerEdge Service and Diagnostic Utilities*
- 1 CD *Dell PowerEdge 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 aucun clavier n'est raccordé.

Le DRAC 5 peut être préinstallé dans le système, ou vous pouvez vous procurer un kit séparé. Si le DRAC 5 est installé sur votre système, consultez la section « [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 plateforme 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. Vérifiez aussi toutes les propriétés RAC Microsoft® Active Directory® associées au DRAC 5 supprimé pour garantir un niveau de sécurité approprié si vous utilisez le 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, effectuez les étapes suivantes :

1. Allumez ou redémarrez votre système.
2. Appuyez sur <Ctrl><E> lorsqu'on vous le demande pendant le test d'auto-diagnostic.

Si votre système d'exploitation commence à se charger avant d'appuyer sur <Ctrl><E>, laissez le système terminer son démarrage, puis redémarrez-le et réessayez.
3. Configurez le NIC.
 - a. À l'aide de la touche représentant une flèche descendante, sélectionnez **Sélection de NIC**.

- b. À l'aide des touches représentant une flèche vers la gauche et une flèche vers la droite, sélectionnez l'une des sélections de NIC suivantes :
- o **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 sur un réseau physique séparé, lui permettant ainsi d'être séparé du trafic de l'application. Cette option est uniquement disponible si une carte DRAC est installée dans le système.
 - o **Partagé** : sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau de périphérique d'accès à distance est complètement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le partage de NIC. Le périphérique d'accès à distance reçoit des données via les NIC 1 et 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.
 - o **Basculement** : sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau de périphérique d'accès à distance est complètement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le partage de NIC. Le périphérique d'accès à distance reçoit des données via les NIC 1 et 2, mais transmet des données seulement via le NIC 1. Si le NIC 1 est défaillant, le périphérique d'accès à distance bascule sur le NIC 2 pour la transmission de toutes les données. Le périphérique d'accès à distance continue à utiliser le NIC 2 pour la transmission des données. Si le NIC 2 est défaillant, le périphérique d'accès à distance bascule sur le NIC 1 pour la transmission de toutes les données.
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 représentant une flèche descendante, sélectionnez **Paramètres LAN**, puis appuyez sur <Entrée>.
 - b. À l'aide des touches représentant une flèche vers la gauche ou la droite, sélectionnez **Source d'adresse IP**.
 - c. À l'aide des touches représentant une flèche vers la gauche ou 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 PowerEdge qui sont configurés avec un seul LAN sur carte mère) peut être configuré avec le regroupement de NIC. Les modes de partage et de 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 du logiciel et de la configuration

Cette section donne une vue d'ensemble de haut niveau des procédures d'installation et de configuration du logiciel 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 des informations supplémentaires sur les composants logiciels du DRAC 5, consultez la section « [Installation du logiciel sur le système géré](#) ».

Installation du logiciel de votre DRAC 5

Pour installer le logiciel de votre DRAC 5, effectuez les étapes suivantes dans l'ordre indiqué :

1. Installez le logiciel sur le système géré. Consultez la section « [Installation du logiciel sur le système géré](#) ».
2. Installez le logiciel sur la station de gestion. Consultez la section « [Installation du logiciel sur la station de gestion](#) ».

Configuration de votre DRAC 5

Pour configurer votre DRAC 5, effectuez les étapes suivantes dans l'ordre indiqué :

1. Sélectionnez un des outils de configuration suivants :
 - 1 Interface Web
 - 1 CLI RACADM
 - 1 Console série/Telnet/SSH

 **AVIS** : L'utilisation de plusieurs outils de configuration de DRAC 5 en même temps peut provoquer des résultats inattendus.

2. Configurez les paramètres réseau du DRAC 5. Consultez la section « [Configuration des paramètres réseau du DRAC 5](#) ».

3. Ajoutez et configurez les utilisateurs du DRAC 5. Consultez la section « [Ajout et configuration des utilisateurs du DRAC 5](#) ».
4. Configurez le navigateur Web pour accéder à l'interface Web. Consultez la section « [Configuration d'un navigateur Web pris en charge](#) ».
5. Désactivez l'option de redémarrage automatique de Windows®. Consultez la section « [Désactivation de l'option de redémarrage automatique de Windows](#) ».
6. Mettez le micrologiciel DRAC 5 à jour. Consultez la section « [Mise à jour du micrologiciel DRAC 5](#) ».
7. Accédez au DRAC 5 via un réseau. Consultez la section « [Accès au DRAC 5 via un réseau](#) ».

Installation du logiciel sur le système géré

L'installation du logiciel sur le système géré est facultative. Si Managed System Software n'est pas installé, vous ne pourrez pas utiliser le RACADM localement et le RAC ne pourra pas saisir l'écran de la dernière panne.

Pour installer le logiciel Managed System Software, installez le logiciel sur le système géré en utilisant le CD *Dell PowerEdge Installation and Server Management*. Pour des instructions sur l'installation de ce logiciel, consultez votre *Guide d'installation rapide*.

Le logiciel Managed System Software installe la version appropriée de Server Administrator de votre choix sur le système géré.

 **REMARQUE :** N'installez pas les logiciels DRAC 5 Management Station Software et DRAC 5 Managed System Software sur le même système.

Si Server Administrator n'est pas installé sur le système géré, vous ne pouvez pas voir l'écran de la dernière panne du système ou utiliser la fonctionnalité **Récupération automatique**.

Pour des informations supplémentaires sur l'écran de la dernière panne, consultez la section « [Affichage de l'écran de la dernière panne du système](#) ».

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 Software. Pour des informations supplémentaires sur l'installation du logiciel Managed System Software, 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 l'interface 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 capturé, l'horloge de **récupération automatique** doit être définie sur 60 secondes ou plus. La valeur 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 éteint.

Désactivation de l'option de redémarrage automatique de Windows

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

Désactivation de l'option de 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. Désélectionnez la case à cocher **Redémarrage automatique**.

5. Cliquez sur **OK** deux fois.

Désactivation de l'option de 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. Désélectionnez la case à cocher **Redémarrage automatique**.

Installation du logiciel sur la station de gestion

Votre système inclut le kit de logiciels de gestion du système de Dell OpenManage. Ce kit inclut, mais sans limitation, les composants suivants :

1. **CD *Installation and Server Management de Dell PowerEdge*** : CD de démarrage qui fournit les outils dont vous avez besoin pour configurer votre système et installer votre système d'exploitation. Ce CD contient les derniers progiciels de gestion du système, notamment les diagnostics Dell OpenManage Server Administrator, Storage Management et les services d'accès à distance.
1. **CD *Dell Systems Management Consoles*** : contient les dernières consoles de gestion de systèmes de Dell, notamment Dell OpenManage IT Assistant.
1. **CD *Dell PowerEdge Service and Diagnostic Utilities*** : fournit les outils dont vous avez besoin pour configurer votre système, ainsi que les dernières versions de micrologiciels, de diagnostics et de pilotes optimisés par Dell pour votre système.
1. **CD *Dell PowerEdge Documentation*** : vous permet d'être informé sur les systèmes, les logiciels de gestion de systèmes, les périphériques et les contrôleurs de RAID.

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 :

1. 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.
1. Pour garantir que les fonctions du visualiseur KVM numérique de Dell fonctionnent correctement, ouvrez les ports suivants sur votre firewall :
 - o Port du clavier et de la souris (le port par défaut est 5900)
 - o Port vidéo (le port par défaut est 5901)

Installation et retrait de RACADM sur une station de gestion Linux

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

 **REMARQUE :** Lorsque vous exécutez **Configuration** sur le CD *Systems Management Consoles*, l'utilitaire RACADM pour tous les systèmes d'exploitation pris en charge est installé sur votre station de gestion.

Installation de RACADM

1. Connectez-vous en tant que racine au système sur lequel vous voulez installer les composants de station de gestion.
2. Si nécessaire, installez le CD *Dell Systems Management Consoles* à l'aide de la commande suivante ou d'une commande semblable :

```
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. Pour plus d'informations sur RACADM, consultez la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

Désinstallation de RACADM

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

```
rpm -e <nom_de_progiciel_racadm>
```

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

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

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

Configuration d'un navigateur Web pris en charge

Les sections suivantes donnent des instructions pour configurer les navigateurs Web pris en charge. Vous trouverez une liste des navigateurs Web pris en charge dans la section « [Navigateurs Web pris en charge](#) ».

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

Si vous êtes connecté 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 accéder à Internet depuis ce serveur.

Pour configurer votre navigateur Web Internet Explorer pour accéder à un serveur proxy, procédez comme suit :

1. Ouvrez une fenêtre de navigateur Web.
2. Cliquez sur **Outils** puis sur **Options Internet**.
3. Dans la fenêtre **Options Internet**, cliquez sur l'onglet **Connexions**.
4. Sous **Paramètres du réseau local**, cliquez sur **Paramètres réseau**.
5. Si la case **Utiliser un serveur proxy** est cochée, 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, 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 pour rétablir une connexion à l'interface Web du DRAC 5.

Navigateurs 32 bits et 64 bits

L'interface Web du DRAC 5 n'est pas prise en charge sur les navigateurs 64 bits. Si vous ouvrez un navigateur 64 bits, accédez à la page **Redirection de console** et essayez d'installer le plug-in, la procédure d'installation échoue. Si cette erreur n'a pas été reconnue et que vous répétez cette procédure, la page **Redirection de console** se charge bien que l'installation de plug-in ait échoué pendant votre premier essai. Ce problème se produit parce que le navigateur enregistre les informations du plug-in dans le répertoire du profil bien que la procédure d'installation de plug-in ait échoué. Pour résoudre ce problème, installez et exécutez un navigateur 32 bits pris en charge et connectez-vous au DRAC 5.

Affichage des 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 :

- 1 Anglais
- 1 Français
- 1 Allemand
- 1 Espagnol
- 1 Japonais
- 1 Chinois simplifié

Pour afficher une version localisée de l'interface Web du DRAC 5 dans Internet Explorer, procédez comme suit :

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 interface graphique utilisateur 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 « locale » 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 », aucun changement 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 changements suivants :

Entrée actuelle :

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

Entrée changée :

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

6. Fermez la session et connectez-vous au 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.

Configuration des propriétés du DRAC 5

Configurez les propriétés du DRAC 5 (réseau, utilisateurs, alertes, etc.) avec l'interface Web ou la RACADM.

Pour des informations supplémentaires sur l'utilisation de l'interface Web, consultez la section « [Accès à l'interface Web](#) ». Pour des informations supplémentaires sur l'utilisation de RACADM dans une connexion série ou Telnet, consultez la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

Configuration des paramètres réseau du DRAC 5

 **AVIS** : 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 :

- 1 Interface Web : consultez la section « [Configuration du NIC du DRAC 5](#) ».
- 1 CLI RACADM : consultez la section « [cfgLanNetworking](#) ».
- 1 Utilitaire de configuration de l'accès à distance de Dell : consultez la section « [Configuration de votre système pour utiliser un DRAC 5](#) ».

 **REMARQUE** : Si vous déployez le DRAC 5 dans un environnement Linux, consultez la section « [Installation de RACADM](#) ».

Ajout et configuration des utilisateurs DRAC 5

Ajoutez et configurez des utilisateurs DRAC 5 avec l'un des outils suivants :

- 1 Interface Web : consultez la section « [Ajout et configuration des utilisateurs du DRAC 5](#) ».
 - 1 CLI RACADM : consultez la section « [cfgUserAdmin](#) ».
-

Mise à jour du micrologiciel DRAC 5

Utilisez l'une des méthodes suivantes pour mettre le micrologiciel DRAC 5 à jour.

- 1 Interface Web : consultez la section « [Mise à jour du micrologiciel DRAC 5 via l'interface Web](#) ».
- 1 CLI RACADM : consultez la section « [fwupdate](#) ».
- 1 Progiciels de mise à jour Dell : consultez le *Guide d'utilisation Dell Update Packages* pour des informations supplémentaires sur l'obtention et l'utilisation de Dell Update Packages dans le cadre de la stratégie de mise à jour de votre système.

Avant de commencer

Avant de mettre à jour votre micrologiciel DRAC 5 à l'aide du RACADM local ou des progiciels Dell Update Packages, procédez comme suit. Sinon, l'opération de mise à jour du micrologiciel risque d'échouer.

1. Installez et activez les pilotes IPMI et de nœuds gérés appropriés.
2. Si votre système fonctionne sous Windows, activez et démarrez les services de l'infrastructure de gestion Windows (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 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 DRAC 5

Pour mettre à jour votre micrologiciel DRAC 5, téléchargez le dernier micrologiciel sur le site Web de support Dell à l'adresse support.dell.com et enregistrez le fichier sur votre système local.

Les composants logiciels suivants sont inclus avec votre progiciel de micrologiciel DRAC 5 :

- 1 Code du micrologiciel compilé du DRAC 5 et données
- 1 Image d'extension de ROM
- 1 Fichiers de données de l'interface Web, JPEG et d'autres interfaces utilisateur
- 1 Fichiers de configuration par défaut

Utilisez la page **Mise à jour de micrologiciel** pour mettre le micrologiciel DRAC 5 au niveau de 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 DRAC 5 via l'interface Web

1. Ouvrez l'interface Web et connectez-vous au système distant.

Consultez la section « [Accès à l'interface Web](#) ».

2. Dans l'arborescence **Système**, cliquez sur **Accès à distance** puis sur l'onglet **Mise 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 **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 DRAC 5.

Suppression du cache de navigateur

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

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

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 :

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

Le [tableau 2-1](#) décrit chaque interface du DRAC 5.

Tableau 2-1. Interfaces du DRAC 5

Interface	Description
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 DRAC 5 et accessible via l'interface NIC d'un navigateur Web pris en charge sur la station de gestion. Vous trouverez une liste des navigateurs Web pris en charge dans la section « Navigateurs Web pris en charge ».
RACADM	Fournit un accès à distance au DRAC 5 à l'aide d'une interface de ligne de commande. RACADM utilise l'adresse IP du système géré pour exécuter des commandes RACADM (option de fonction d'accès à distance <code>racadm [-r]</code>). REMARQUE : La fonction d'accès à distance <code>racadm</code> n'est prise en charge que sur les stations de gestion. Consultez la section « Navigateurs Web pris en charge » pour plus d'informations. REMARQUE : Quand vous utilisez la fonction d'accès à distance <code>racadm</code> , vous devez avoir le droit d'écrire dans les fichiers où se trouvent les sous-commandes <code>racadm</code> avec des opérations de fichiers, comme par exemple : <code>racadm getconfig -f <nom de fichier></code> ou :

	<code>sous-commandes racadm sslcertupload -t 1 -f c:\cert\cert.txt</code>
Console Telnet	Fournit l'accès via le DRAC 5 au port RAC du serveur et les 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 meilleure sécurité.
Interface IPMI	Fournit l'accès via le DRAC 5 aux fonctionnalités de gestion de base du système distant. L'interface inclut IPMI sur le LAN, IPMI sur communication série et Communication série sur le LAN. Consultez le <i>Guide d'utilisation du contrôleur de gestion de la carte mère de Dell OpenManage</i> 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.

Vous trouverez une liste des navigateurs Web pris en charge dans la section « [Navigateurs Web pris en charge](#) ».

Pour accéder au DRAC 5 à l'aide d'un navigateur Web pris en charge, consultez la section « [Accès à l'interface Web](#) ».

Pour accéder à l'interface d'accès à distance du DRAC 5 avec Server Administrator, lancez Server Administrator. Dans l'arborescence du système située sur le panneau de 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.

Pour des informations sur l'accès au DRAC 5 avec le RACADM, consultez la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

Configuration d'IPMI

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

- 1 IPMI sur le LAN
- 1 IPMI sur communications série
- 1 Communications série sur le LAN

Le DRAC5 est compatible IPMI 2.0. Vous pouvez configurer l'interface IPMI du DRAC à l'aide de votre navigateur ; à l'aide d'un utilitaire open source, comme *ipmitool* ; à l'aide de l'environnement IPMI Dell OpenManage, *ipmish* ; ou à l'aide de 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 Dell à l'adresse support.dell.com.

Pour plus d'informations sur l'utilisation de RACADM, consultez la section « [Utilisation de RACADM](#) ».

Configuration d'IPMI via l'interface Web

1. Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge. Consultez la section « [Accès à l'interface Web](#) ».
2. Configurez IPMI sur le LAN.
 - a. Dans l'arborescence **Système**, cliquez sur **Accès à distance**.
 - 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 le 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 changements**.

- e. Configurez la clé de cryptage de canal LAN IPMI, si nécessaire.

 **REMARQUE :** L'interface 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 changements**.

 **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 **Systeme**, cliquez sur **Accès à distance**.
 - b. Dans l'onglet **Configuration**, cliquez sur **Communications série sur le LAN**.
 - c. Sur la page **Configuration des communications série sur le LAN**, sélectionnez **Activation des communications série sur le LAN**.
 - d. Mettez à jour le débit en bauds de SOL IPMI.

 **REMARQUE :** Pour rediriger la console série sur le 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 changements**.
 - f. Mettez à jour le **Privilèges obligatoires minimum**. Cette propriété définit le privilège utilisateur minimum qui est nécessaire pour utiliser la fonctionnalité **Communications série sur le LAN**.

Cliquez sur le menu déroulant **Limite du niveau de privilège du canal**, sélectionnez **Utilisateur**, **Opérateur** ou **Administrateur**.
 - g. Cliquez sur **Appliquer les changements**.
4. Configurez les communications série IPMI.
 - 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 **Communications série IPMI**, cliquez sur le menu déroulant **Paramètre du mode de connexion** et sélectionnez le mode approprié.
 - c. Configurez le débit en bauds des communications série IPMI.

Cliquez sur le menu déroulant **Débit en bauds**, sélectionnez le débit en bauds approprié et cliquez sur **Appliquer les changements**.
 - 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 changements**.
 - f. Assurez-vous que MUX série est correctement configuré dans le programme de configuration du BIOS du système géré.
 - o Redémarrez votre système.
 - o Pendant le test d'autodiagnostic, appuyez sur <F2> pour accéder au programme de configuration du BIOS.
 - o Allez à **Serial Communication (Communications série)**.
 - o Dans le menu **Serial Connection (Connexion série)**, assurez-vous que le **External Serial Connector (Connecteur série externe)** est défini sur **Remote Access Device (Périphérique d'accès à distance)**.
 - o Enregistrez et quittez le programme de configuration du BIOS.
 - o Redémarrez votre système.

Si Communications série IPMI est en mode terminal, vous pouvez configurer les paramètres supplémentaires suivants :

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

Pour plus d'informations sur ces propriétés, consultez la spécification IPMI 2.0.

Configuration d'IPMI via la CLI RACADM

1. Connectez-vous au système distant à l'aide d'une des interfaces RACADM. Voir « [Utilisation de RACADM](#) ».
2. Configurez IPMI sur le 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 le LAN. Pour plus d'informations, consultez les spécifications d'IPMI 2.0.

- a. Mettez à jour les privilèges de canal IPMI.

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

```
racadm config -g cfgIpmlan -o cfgIpmlanPrivilegeLimit <niveau>
```

où <niveau> correspond à :

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

Par exemple, pour configurer le privilège de canal LAN IPMI sur 2 (utilisateur), tapez la commande suivante :

```
racadm config -g cfgIpmlan -o cfgIpmlanPrivilegeLimit 2
```

- b. Configurez la clé de cryptage de canal LAN IPMI, si nécessaire.

 **REMARQUE :** L'interface 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 cfgIpmlan -o cfgIpmlanEncryptionKey <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 cfgIpmlan -o cfgIpmlanSolEnable 1
```

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

Le niveau de privilège minimum de SOL IPMI détermine le privilège minimum requis pour activer le SOL IPMI. Pour plus d'informations, consultez la spécification IPMI 2.0.

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

```
racadm config -g cfgIpmlan -o cfgIpmlanSolMinPrivilege <niveau>
```

où <niveau> correspond à :

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

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

```
racadm config -g cfgIpmlan -o cfgIpmlanSolMinPrivilege 2
```

- b. Mettez à jour le débit en bauds de SOL IPMI.

 **REMARQUE :** Pour rediriger la console série sur le 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 cfgIpmlan -o cfgIpmlanSolBaudRate <débit_en_bauds>
```

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

Par exemple :

```
racadm config -g cfgIpmlan -o cfgIpmlanSolBaudRate 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'identifiant unique de l'utilisateur.

4. Configurez les communications série IPMI.

- a. Remplacez le mode de connexion série IPMI par le paramètre approprié.

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

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

- b. Configurez le débit en bauds des communications série IPMI.

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 du matériel série IPMI.

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 série IPMI.

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

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <niveau>
```

où <niveau> correspond à :

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

Par exemple, pour configurer les privilèges de canal série IPMI 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.

- o Redémarrez votre système.
- o Pendant le test d'autodiagnostic, appuyez sur <F2> pour accéder au programme de configuration du BIOS.
- o Allez à **Serial Communication (Communications série)**.
- o Dans le menu **Serial Connection (Connexion série)**, assurez-vous que le **External Serial Connector (Connecteur série externe)** est défini sur **Remote Access Device (Périphérique d'accès à distance)**.
- o Enregistrez et quittez le programme de configuration du BIOS.
- o Redémarrez votre 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` :

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

Pour plus d'informations sur ces propriétés, consultez la spécification IPMI 2.0.

Configuration des événements sur plateforme

La configuration des événements sur plateforme offre un outil de configuration du périphérique d'accès à distance pour effectuer les actions sélectionnées sur certains messages d'événement. Ces actions incluent le redémarrage, le cycle d'alimentation, la mise hors tension et le déclenchement d'une alerte (interruption des événements sur plateforme [PET] et/ou e-mail).

Les événements sur plateforme pouvant être filtrés incluent :

- 1 Panne de capteur de ventilateur
- 1 Avertissement des capteurs de batterie
- 1 Panne de capteur de batterie
- 1 Panne du capteur discret de tension
- 1 Avertissement des capteurs de température

- 1 Panne de capteur de température
- 1 Détection d'une intrusion dans le châssis
- 1 Dégradation de la redondance
- 1 Perte de la redondance
- 1 Avertissement concernant un processeur
- 1 Panne de processeur
- 1 Processeur absent
- 1 Avertissement concernant PS/VRM/D2D
- 1 Panne de PS/VRM/D2D
- 1 Bloc d'alimentation absent
- 1 Erreur dans le journal du matériel
- 1 Récupération automatique du système

Lorsqu'un événement sur plateforme 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 plateforme (PEF) dans la liste des filtres d'événements sur plateforme 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 plateforme est aussi configuré pour effectuer une action (ex. : redémarrage du système), l'action est effectuée.

Configuration des filtres d'événements sur plateforme (PEF)

Configurez vos filtres d'événements sur plateforme avant de configurer les interruptions d'événement sur plateforme ou les paramètres d'alerte par e-mail.

Configuration du PEF via l'interface utilisateur Web

1. Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge. Consultez la section « [Accès à l'interface Web](#) ».
2. Cliquez sur l'onglet **Gestion des alertes** et sur **Événements sur plateforme**.
3. Activez les alertes globales.
 - a. Cliquez sur **Gestion des alertes** et sélectionnez **Événements sur plateforme**.
 - b. Cochez la case **Activer les alertes de filtre d'événements sur plateforme**.
4. Dans **Configuration des filtres d'événements de la plateforme**, cochez la case **Activer les alertes de filtre d'événements sur plateforme** et cliquez sur **Appliquer les changements**.
5. Dans **Liste des filtres d'événements de la plateforme**, double-cliquez sur le filtre que vous voulez configurer.
6. Sur la page **Définition d'événements sur plateforme**, effectuez les sélections appropriées et cliquez sur **Appliquer les changements**.

 **REMARQUE :** L'option **Génération d'une alerte** doit être activée pour qu'une alerte soit envoyée à une destination configurée et valide (PET ou par e-mail).

Configuration du PEF via 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 configurée sur 1 (Activé) ou 0 (Désactivé).

Par exemple, pour activer le PEF avec l'index 5, tapez la commande suivante :

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. Configurez vos actions PEF.

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

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <action>
```

où les bits de valeur d'<action> sont les suivants :

- 1 <action> bit de valeur 0 - 1 = action d'alerte activée, 0 = alerte désactivée
- 1 <action> bit de valeur 1 - 1 = mise hors tension ; 0 = pas de mise hors tension
- 1 <action> bit de valeur 2 - 1 = redémarrage ; 0 = pas de redémarrage
- 1 <action> bit de valeur 3 - 1 = cycle d'alimentation ; 0 = pas de cycle d'alimentation

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 au redémarrage.

Configuration de PET

Configuration de PET via l'interface utilisateur Web

1. Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge. Consultez la section « [Accès à l'interface Web](#) ».
2. Vérifiez si vous avez suivi les procédures décrites dans la section « [Configuration de 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 et cliquez sur **Appliquer les changements**.
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 changements**.
 - e. Cliquez sur **Envoyez l'interruption test** pour tester l'alerte configurée (si nécessaire).

 **REMARQUE** : Votre compte utilisateur doit avoir l'autorisation de **tester les alertes** pour effectuer cette procédure. Consultez le [tableau 4-8](#).

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

Configuration de PET via la CLI RACADM

1. Activez vos alertes globales.

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

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

2. Activez PET.

À l'invite de commande, tapez la commande suivante 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 configurée sur 1 (Activé) ou 0 (Désactivé).

Par exemple, pour activer 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 plateforme.

- Configurez la chaîne de nom de communauté.

À l'invite de commande, tapez :

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Nom>
```

Configuration des alertes par e-mail

Configuration d'alertes par e-mail via l'interface utilisateur Web

- Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge. Consultez la section « [Accès à l'interface Web](#) ».
- Vérifiez si vous avez suivi les procédures décrites dans la section « [Configuration de PEF via l'interface utilisateur Web](#) ».
- Configurez vos paramètres d'alerte par e-mail.
 - Dans l'onglet **Gestion des alertes**, cliquez sur **Paramètres d'alertes par e-mail**.
 - Dans **Adresse du serveur SMTP (e-mail)**, configurez le champ **Adresse IP du serveur SMTP (e-mail)** avec les informations appropriées et cliquez sur **Appliquer les changements**.
- Configurez votre destination d'alerte par e-mail.
 - Dans la colonne **Numéro d'alerte par e-mail**, cliquez sur un numéro d'alerte par e-mail.
 - Vérifiez si la case **Activer l'alerte par e-mail** est cochée.
 - Dans le champ **Adresse e-mail de destination**, tapez une adresse e-mail valide.
 - Dans le champ **Description de l'e-mail**, entrez une description (si nécessaire).
 - Cliquez sur **Appliquer les changements**.
 - Cliquez sur **Envoyer l'e-mail test** pour tester l'alerte par e-mail configurée (si nécessaire).

 **REMARQUE** : Votre compte utilisateur doit avoir l'autorisation de **tester les alertes** pour effectuer cette procédure. Consultez le [tableau 4-8](#).

 - Répétez les étapes [a](#) à [g](#) pour les autres paramètres d'alerte par e-mail.
- Activez les alertes globales.
 - Cliquez sur **Gestion des alertes** et sélectionnez **Événements sur plateforme**.
 - Cochez la case **Activer les alertes de filtre d'événements sur plateforme**.

Configuration d'alertes par e-mail via la CLI RACADM

- Activez vos alertes globales.

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

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

- Activez les alertes par e-mail.

À l'invite de commande, tapez la commande suivante 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 configurée 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
```

- Configurez vos paramètres d'e-mail.

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

```
racadm config -g cfgEmailAlert -O cfgEmailAlertAddress -i 1 <adresse_e-mail>
```

où 1 est l'index de destination d'e-mail et <adresse_e-mail> l'adresse e-mail de destination qui reçoit les alertes d'événement sur plateforme.

Pour configurer un message personnalisé, à l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgEmailAlert -O cfgEmailAlertCustomMsg -i 1 <message_personnalisé>
```

où 1 est l'index de destination d'e-mail et <message_personnalisé> le message personnalisé.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration et utilisation de la console de ligne de commande DRAC 5

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Fonctionnalités de la console de ligne de commande](#)
- [Activation et configuration du système géré pour utiliser une console série ou Telnet](#)
- [Utilisation du protocole Secure Shell \(SSH\)](#)
- [Activation d'options de sécurité supplémentaires de DRAC 5](#)
- [Connexion au système géré via le port série local ou une station de gestion Telnet \(système client\)](#)
- [Connexion du câble DB-9 pour la console série](#)
- [Configuration du logiciel d'émulation de terminal de la station de gestion](#)
- [Utilisation d'une console série ou Telnet](#)

Cette section fournit des informations sur les fonctionnalités de la console de ligne de commande du DRAC 5 (ou *console série/Telnet/SSH*) et explique comment configurer votre système de manière à pouvoir effectuer des actions de gestion de systèmes via la console.

Fonctionnalités de la console de ligne de commande

Le DRAC 5 prend en charge les fonctionnalités de redirection de console série et Telnet suivantes :

- 1 Une connexion de client série et un maximum de quatre connexions de clients Telnet simultanées
- 1 Jusqu'à quatre connexions client SSH simultanées
- 1 L'accès aux consoles du système géré via le port série du système et le NIC du DRAC 5
- 1 Les commandes de console qui vous permettent de mettre sous tension, mettre hors tension, effectuer un cycle d'alimentation, afficher les journaux ou configurer le DRAC 5
- 1 La prise en charge de la commande **RACADM** qui est utile pour les scripts
- 1 La modification et l'historique de la ligne de commande
- 1 La commande série **connect com2**, envoyée via un port série (y compris le BIOS et le système d'exploitation) pour la connexion à la console texte du système géré, son affichage et l'interaction

 **REMARQUE** : Si vous exécutez Linux sur le système géré, la commande série **connect com2** fournit une vraie interface de flux de données de console Linux.

- 1 Contrôle du délai d'expiration de la session sur toutes les interfaces de console

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**, ce qui suit doit être configuré correctement :

- 1 Le paramètre **Serial Communication (Communications série)** → **Serial Port (Port série)** dans le programme **Configuration du BIOS**.
- 1 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 de **configuration du BIOS**.

 **REMARQUE** : Vous devez configurer le programme de **configuration du système** en association avec la commande **connect com2**.

1. Allumez ou redémarrez votre système.
2. Appuyez sur <F2> dès que le message suivant s'affiche :

<F2> = System Setup

<F2> = Configuration du système)

3. Faites défiler la fenêtre et sélectionnez **Serial Communication (Communication série)** en appuyant sur <Entrée>.
4. Définissez l'écran **Serial Communication (Communication série)** avec les paramètres suivants :
External Serial Connector — Remote Access Device (Connecteur série externe : périphérique d'accès à distance)
Redirection After Boot — Disabled (Redirection après démarrage : désactivée)
5. Appuyez sur <Échap> pour quitter le programme de **configuration du système** et terminer la configuration du programme de **configuration du système**.

Utilisation de l'interface série d'accès à distance

Lorsque vous établissez une connexion série sur le périphérique RAC, les interfaces suivantes sont disponibles :

- 1 Interface série IPMI
- 1 Interface série RAC

Interface série IPMI

Dans l'interface série IPMI, les modes suivants sont disponibles :

- 1 **Mode terminal IPMI** : prend en charge les commandes ASCII qui sont envoyées à partir d'un terminal série. Le jeu de commande est limité à un nombre limité de commandes (notamment le contrôle de l'alimentation) et prend en charge les commandes IPMI brutes qui sont entrées sous forme de caractères ASCII hexadécimaux.
- 1 **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 RACADM, effectuez les étapes suivantes :

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>
```

Consultez la section « [Définitions de groupes et d'objets de la base de données des propriétés du DRAC 5](#) » pour plus d'informations.

Interface série RAC

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 ignore 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
```

Consultez la section « [cfgSerialConsoleEnable \(lecture/écriture\)](#) » pour plus d'informations.

Le [tableau 3-1](#) fournit les paramètres d'interface série.

Tableau 3-1. Paramètres d'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 de Linux (GRand Unified Bootloader). Il faudra faire des modifications du même genre si vous utilisez un chargeur de démarrage différent.

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 fin de la ligne de noyau :

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

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

Le [tableau 3-2](#) fournit un modèle de fichier `/etc/grub.conf` qui illustre les changements décrits dans cette procédure.

Tableau 3-2. Modèle de fichier : `/etc/grub.conf`

```
# grub.conf generated by anaconda
# (grub.conf généré par anaconda)
#
# Note that you do not have to rerun grub after making changes
# to this file
# (Notez que vous n'avez pas besoin de redémarrer grub après avoir effectué
# les changements dans ce fichier)
# NOTICE: You do not have a /boot partition. This means that
# all kernel and initrd paths are relative to /, e.g.
# (AVIS : Vous n'avez pas de partition d'amorçage /. Cela signifie
# que tous les noyaux et chemins initrd concernent /, ex.)
#
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sdal
# initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

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

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

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 de 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 série RAC, ajoutez la ligne suivante à toutes les options :

```
console=ttyS1,57600
```

Le [tableau 3-2](#) affiche `console=ttyS1,57600` ajouté à la première option uniquement.

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

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

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

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

Le [tableau 3-3](#) illustre un modèle de fichier avec la nouvelle ligne.

Tableau 3-3. Modèle de fichier : /etc/inittab

```
#
# inittab This file describes how the INIT process should set up
# the system in a certain run-level.
# (inittab Ce fichier décrit comment le processus d'initialisation doit
# configurer le système pour un certain niveau d'exécution.)
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
# (Auteur : Miquel van Smoorenburg
# Modifié pour RHS Linux par Marc Ewing et 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)
#
# (Niveau d'exécution par défaut. Les niveaux d'exécution utilisés par RHS sont les suivants :
# 0 - Arrêt (ne configurez PAS initdefault sur ce niveau)
# 1 - Mode mono-utilisateur
# 2 - Multi-utilisateur, sans NFS (semblable à 3, si vous n'avez pas de
# connexion réseau)
# 3 - Mode multi-utilisateur intégral
# 4 - Non utilisé
# 5 - X11
# 6 - Redémarrage (ne configurez PAS initdefault sur ce niveau)
#
id:3:initdefault:

# System initialization
# (Initialisation du système).
si:sysinit:/etc/rc.d/rc.sysinit

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

# Things to run in every runlevel
# (Éléments à exécuter pour chaque mode d'exécution).
ud:once:/sbin/update

# Trap CTRL-ALT-DELETE
# (Interruption CTRL-ALT-SUPPR)
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.
#
# (Quand l'onduleur indique une panne de courant, vous avez quelques
# minutes de courant restant. Arrêtez dans 2 minutes.
# Ceci part du principe que l'appareil est alimenté et que votre
# onduleur est raccordé et opérationnel.)
pf:powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
# (Si l'alimentation a été restaurée avant l'arrêt, annulez cette opération.)
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
# (Exécute gettys en modes d'exécution standard)
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
#
# (Exécute xdm en mode d'exécution 5
# xdm est désormais un service séparé)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

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

```
ttyS1
```

Le [tableau 3-4](#) illustre un modèle de fichier avec la nouvelle ligne.

Tableau 3-4. Modèle 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 sur le DRAC 5

Vous pouvez activer la console série/Telnet/SSH localement ou à distance.

Activation locale de la console série/Telnet/SSH

 **REMARQUE :** Vous (l'utilisateur actuel) devez avoir le droit de **configurer le DRAC 5** pour pouvoir effectuer les étapes de cette section.

Pour activer la console série/Telnet/SSH depuis le système géré, tapez les commandes locales de RACADM 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
```

Vous trouverez des informations détaillées sur l'utilisation de **RACADM**, des commandes **série/Telnet/SSH**, et des commandes **RACADM** dans la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

Activation à distance de la console série/Telnet/SSH

Pour activer la console série/Telnet/SSH à distance, tapez les commandes à distance **RACADM** suivantes à partir d'une invite de commande :

```
racadm -u <nom d'utilisateur> -p <mot de passe> -r <adresse IP du DRAC 5> config -g cfgSerial cfgSerialConsoleEnable 1
```

```
racadm -u <nom d'utilisateur> -p <mot de passe> -r <adresse IP du DRAC 5> config -g cfgSerial cfgSerialTelnetEnable 1
```

```
racadm -u <nom d'utilisateur> -p <mot de passe> -r <adresse IP du DRAC 5> config -g cfgSerial cfgSerialSshEnable 1
```

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 **RACADM config** 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.

Vous trouverez une liste complète des commandes série/Telnet/SSH et de CLI **RACADM** dans la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

Utilisation de RACADM localement

Pour utiliser les commandes RACADM localement, tapez les commandes suivantes 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 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 RACADM à distance. Sinon, la session RACADM expire et le message suivant apparaît :

```
Unable to connect to RAC at specified IP address.
```

```
(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 lors d'une invite de commande sur une station de gestion :

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

Affichage des paramètres de configuration

Le [tableau 3-5](#) 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 3-5. Affichage des paramètres de configuration

Action	Commande
Énumération des groupes disponibles.	racadm getconfig -h
Affichage des 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
Affichage des 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 du protocole Secure Shell (SSH)

Il est essentiel que les périphériques de votre système et la gestion des périphériques soient sécurisés. Les périphériques connectés intégrés sont au cœur de nombreux processus d'affaires. Si ces périphériques sont compromis, les affaires du client peuvent être menacées, 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 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 devrait 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 clés 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 avec la propriété `cfgSsnMgtSshIdleTimeout` comme indiqué dans la section « [Définitions de groupes et d'objets de la base de données des propriétés 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`, consultez la section « [Définitions de groupes et d'objets de la base de données des propriétés du DRAC 5](#) ».

L'implémentation SSH du DRAC 5 prend en charge plusieurs projets de cryptographie, comme illustré dans le [tableau 3-6](#).

Tableau 3-6. Schémas de cryptographie

Type de schéma	Schéma
Cryptographie asymétrique	Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 par NIST
Cryptographie symétrique	<ul style="list-style-type: none">1 AES256-CBC1 RIJNDAEL256-CBC1 AES192-CBC1 RIJNDAEL192-CBC1 AES128-CBC1 RIJNDAEL128-CBC1 BLOWFISH-128-CBC1 3DES-192-CBC1 ARCFOUR-128
Intégrité du message	<ul style="list-style-type: none">1 HMAC-SHA1-1601 HMAC-SHA1-961 HMAC-MD5-1281 HMAC-MD5-96
Authentification	<ul style="list-style-type: none">1 Mot de passe

 **REMARQUE :** SSHV1 n'est pas pris en charge.

Activation d'options de sécurité supplémentaires de DRAC 5

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

- 1 Filtrage des adresses IP (IPRange) : définit une plage spécifique d'adresses IP auxquelles peut accéder le DRAC 5.
- 1 Blocage des adresses IP : limite le nombre d'échecs de tentatives de connexion 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 d'objet> <valeur>
```

De plus, utilisez ces fonctionnalités en association avec les valeurs de délai d'attente de la session appropriée 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 uniquement un accès au DRAC 5 à partir des clients ou 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 suivantes `cfgRacTuning` :

- 1 `cfgRacTuneIpRangeAddr`
- 1 `cfgRacTuneIpRangeMask`

La propriété `cfgRacTuneIpRangeMask` est appliquée à l'adresse IP entrante et aux propriétés `cfgRacTuneIpRangeAddr`. Si les résultats des deux propriétés sont identiques, la demande d'ouverture de session entrante accède 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.

Consultez la section « [Définitions de groupes et d'objets de la base de données des propriétés du DRAC 5](#) » pour une liste complète des propriétés `cfgRacTune`.

Tableau 3-7. Propriétés de filtrage des adresses IP (IpRange)

Propriété	Description
<code>cfgRacTuneIpRangeEnable</code>	Active la fonctionnalité de contrôle de plage IP.
<code>cfgRacTuneIpRangeAddr</code>	Détermine le format binaire d'adresse IP autorisé, en fonction des 1 dans le masque de sous-réseau. Cette propriété correspond à l'opérateur AND avec <code>cfgRacTuneIpRangeMask</code> 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.
<code>cfgRacTuneIpRangeMask</code>	Définit les positions binaires significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau, où les bits de plus fort poids sont tous des 1 avec une transition simple à tous les zéros dans les bits inférieurs.

Activation du filtrage IP

Voici un exemple de commande pour la configuration du filtrage IP.

Consultez la section « [Utilisation de RACADM](#) » pour plus d'informations sur RACADM et les commandes RACADM.

 **REMARQUE :** Les commandes RACADM suivantes bloquent toutes les adresses IP sauf 192.168.0.57)

Pour restreindre l'ouverture de session à une seule adresse IP (par exemple, 192.168.0.57), utilisez le masque complet, comme illustré ci-dessous.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

Pour restreindre les ouvertures de session à un petit ensemble de quatre adresses IP adjacentes (par exemple, 192.168.0.212 à 192.168.0.215), sélectionnez tous 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 255.255.255.252
```

Instructions concernant le filtrage IP

Observez les instructions suivantes lorsque vous activez le filtrage IP :

- 1 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 plus faible poids.
- 1 Utilisez l'adresse de base de la plage de votre choix comme valeur de `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 empêche l'adresse de se connecter au DRAC 5 pendant une période prédéfinie.

Le paramètre de blocage IP utilise les fonctionnalités de groupe `cfgRacTuning` telles que :

- 1 Le nombre d'échecs d'ouverture de session autorisés ([cfgRacTuneIpBlkFailcount](#))
- 1 L'intervalle de temps en secondes au cours duquel ces échecs doivent se produire ([cfgRacTuneIpBlkFailWindow](#))
- 1 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 ([cfgRacTuneIpBlkPenaltyTime](#))

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 se connecte 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.

Consultez la section « [Définitions de groupes et d'objets de la base de données des propriétés du DRAC 5](#) » pour une liste complète des propriétés `cfgRacTune`.

Le [tableau 3-8](#) énumère les paramètres définis par l'utilisateur.

Tableau 3-8. 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	Configure le nombre d'échecs d'ouverture de session à partir d'une adresse IP avant que les tentatives d'ouverture de session ne soient rejetées.
cfgRacTuneIpBlkFailWindow	Intervalle de temps en secondes pendant lequel les échecs d'ouverture de session sont comptés. Lorsque le nombre d'échecs dépasse cette limite, le compteur est remis à zéro.
cfgRacTuneIpBlkPenaltyTime	Définit l'intervalle de temps en secondes au cours duquel toutes les tentatives d'ouverture de session à partir d'une adresse IP avec des échecs excessifs sont rejetées.

Activation du blocage IP

L'exemple suivant empêche une adresse IP client d'ouvrir une session pendant cinq minutes si ce client a échoué 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
```

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 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 (consultez la section « [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. Consultez la section « [Configuration du logiciel d'émulation de terminal sur la station de gestion](#) » pour plus d'informations.

Les sous-sections suivantes expliquent comment connecter votre station de gestion au système géré à l'aide des méthodes suivantes :

- 1 Un port série externe du système à l'aide du logiciel de terminal et d'un câble simulateur de modem
- 1 Une connexion Telnet à l'aide du logiciel terminal via le NIC du système géré du DRAC 5 ou le NIC partagé

Connexion du câble DB-9 pour la console série

Pour accéder au système géré en utilisant une console texte série, vous devez raccorder un câble simulateur de modem 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 3-9](#).

 **REMARQUE :** Le câble DB-9 peut aussi être utilisé pour la redirection de console de texte du BIOS.

Tableau 3-9. Brochage requis pour le câble null modem 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 émettre)	8	7
SG (Terre du signal)	5	5
DSR (Poste 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 :

- 1 Linux Minicom dans un terminal Xterm
- 1 HyperTerminal Private Edition (version 6.3) de Hilgraeve
- 1 Linux Telnet dans un terminal Xterm
- 1 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 principaux. Utilisez les informations de la section « [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 à 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 <Minicom nom du fichier de configuration>` et passez à l'[étape 17](#).
4. À l'invite de commande Xterm, tapez `minicom -s`.
5. Sélectionnez **Configuration du port série** et appuyez sur <Entrée>.
6. Appuyez sur <a> et sélectionnez le périphérique série approprié (`/dev/ttySo`, par exemple).
7. Appuyez sur <e> et définissez l'option **Bits par seconde/Parité/Bits** sur `57600 8N1`.
8. Appuyez sur <f>, définissez **Contrôle matériel du débit** sur **Oui** et définissez **Contrôle logiciel du débit** 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 de **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 de **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 <Minicom nom du fichier de configuration>`.
17. Pour agrandir la fenêtre de Minicom à 80 x 25, faites glisser le coin de la fenêtre.
18. Pour quitter Minicom, appuyez sur <Ctrl+a>, <z>, <x>.

 **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 dans l'invite de commande : `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 Minicom requis pour l'émulation de console série

Utilisez le [tableau 3-10](#) pour configurer les versions de Minicom.

Tableau 3-10. Paramètres Minicom pour l'émulation de console série

Description du paramètre	Paramètre requis
Bits par seconde/Parité/Bits	57600 8N1
Contrôle matériel du débit	Oui
Contrôle logiciel du débit	Non
Émulation de terminal	ANSI
Configuration de la numérotation du modem et des paramètres	Effacez les paramètres de <code>init</code> , <code>reset</code> , <code>connect</code> et <code>hangup</code> 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, effectuez les étapes suivantes :

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 raccordé le câble null modem DB-9 et cliquez sur **OK**.
4. Configurez les paramètres de port COM selon le [tableau 3-11](#).
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 3-11. Paramètres de 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 de 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 :

1. Lorsque vous utilisez la commande `connect com2` via une console Telnet pour afficher les écrans de configuration du système, définissez le type de terminal sur **ANSI** dans le programme de configuration du système et pour la session Telnet.
1. 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 Telnet avec Linux, effectuez les étapes suivantes :

1. Démarrez une nouvelle session Xterm.

À l'invite de commande, tapez `xterm &`

2. À l'aide du curseur de la souris, cliquez dans l'angle inférieur droit de la fenêtre XTerm et redimensionnez la fenêtre à 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 Telnet Microsoft 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. Mais, la plupart des clients Telnet Microsoft et Linux peuvent être configurés pour utiliser la touche <Retour> arrière.

Pour configurer les clients Telnet Microsoft à utiliser la touche <Retour> arrière, effectuez les étapes suivantes :

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><J>.

3. À l'invite, tapez :

```
set bsasdel
```

Le message suivant apparaît :

```
Backspace will be sent as delete.
```

(Le retour arrière sera envoyé comme supprimer.)

Pour configurer une session Telnet Linux à utiliser la touche <Retour> arrière, effectuez les étapes suivantes :

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.

Pour des informations supplémentaires sur les commandes **série/Telnet/SSH** ainsi que sur la CLI RACADM, consultez la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

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 de caractères dans une session Telnet DRAC 5. Ce problème peut se produire sous forme d'ouverture de session gelée 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 le correctif 824810 à partir du site Web de support de Microsoft à l'adresse support.microsoft.com. Consultez l'article 824810 de la base de connaissances 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 pour Windows Services for UNIX® 3.5 de Microsoft. Vous pouvez télécharger Windows Services for UNIX 3.5 à l'adresse www.microsoft.com/windows/sfu/downloads/default.asp.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration du DRAC 5 via l'interface utilisateur Web

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Accès à l'interface Web](#)
- [Configuration du NIC du DRAC 5](#)
- [Ajout et configuration des utilisateurs DRAC 5](#)
- [Configuration et gestion de certificats Active Directory \(schémas standard et étendu\)](#)
- [Sécurisation des communications DRAC 5 via SSL et des certificats numériques](#)
- [Configuration des modes série et terminal](#)
- [Configuration des communications série sur le LAN](#)
- [Configuration des services](#)
- [Questions les plus fréquentes](#)

DRAC 5 est doté d'une interface Web et de RACADM (une interface de ligne de commande) qui vous permet de configurer les propriétés et les utilisateurs DRAC 5, d'effectuer des tâches de gestion à distance et de dépanner un système (géré) distant 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 vous donne des liens vers des informations connexes.

Toutes les tâches de configuration de l'interface Web peuvent aussi se faire via RACADM. Vous trouverez une liste de toutes les commandes série/Telnet/SSH et RACADM qui peuvent être utilisées pour effectuer chaque tâche en mode texte dans la section « [Utilisation de l'interface de ligne de commande RACADM](#) ».

Consultez l'aide en ligne de votre DRAC 5 pour des informations contextuelles sur chaque page d'interface Web.

Accès à l'interface Web

Pour accéder à l'interface Web du DRAC 5, effectuez les étapes suivantes :

1. Ouvrez une fenêtre de navigateur Web prise en charge.

Consultez la section « [Navigateurs Web pris en charge](#) » pour plus d'informations.

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 d'ouverture de session du DRAC 5 apparaît.

Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur DRAC 5 ou utilisateur 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 l'autorisation de vous **connecter au DRAC 5**.

Pour ouvrir une session, effectuez les étapes suivantes.

1. Dans le champ **Nom d'utilisateur**, tapez :

- 1 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.

- 1 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\jean_dupont` ou `jean_dupont@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 distingue les majuscules des minuscules.

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 Web.

 **REMARQUE :** Le bouton **Fermer la session** n'apparaît pas tant qu'une session n'a pas été ouverte.

 **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 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 for Internet Explorer à partir du site Web de support de Microsoft, à l'adresse : support.microsoft.com.

Configuration du NIC du DRAC 5

Configuration des paramètres réseau et LAN IPMI

 **REMARQUE :** Vous devez avoir le droit de **configurer le DRAC 5** pour effectuer les étapes suivantes.

 **REMARQUE :** La plupart des serveurs DHCP nécessitent un serveur pour stocker un jeton d'identifiant client dans sa table de réservation. Le client (DRAC 5, par exemple) doit fournir ce jeton pendant la négociation DHCP. Pour les RAC, le DRAC 5 fournit l'option d'identifiant client à l'aide d'un numéro (0) d'interface à un octet suivi par une adresse MAC à six octets.

 **REMARQUE :** Si le système géré de votre DRAC 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 **Système**, cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.
3. Sur la page **Configuration réseau**, configurez les paramètres NIC du DRAC 5.

Le [tableau 4-1](#) et le [tableau 4-2](#) décrivent les **paramètres réseau** et les **paramètres IPMI** sur la page **Configuration réseau**.

4. Lorsque vous avez terminé, cliquez sur **Appliquer les changements**.
5. Cliquez sur le bouton approprié sur la page **Configuration réseau** pour continuer. Consultez le [tableau 4-3](#).

Tableau 4-1. Paramètres réseau

Paramètre	Description
Sélection de NIC	Affiche le mode NIC sélectionné (Dédié , Partagé avec basculement ou Partagé). Le paramètre par défaut est Dédié .
Adresse MAC	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 d'hôte (DHCP). Le fait de sélectionner la case à cocher 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 nous n'avez qu'un serveur DNS, vous devez entrer 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 DRAC DNS	N'affiche le nom du DRAC 5 que si Enregistrer le DRAC 5 auprès du DNS est sélectionné. Par défaut, le nom DRAC 5 est RAC-- <i>numéro de service, numéro de service</i> 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 communiquant avec le routeur ou le concentrateur le plus proche (Activé) ou de définir le mode duplex et la vitesse du réseau manuellement (Désactivé).
Vitesse du réseau	Définit une vitesse du réseau de 100 Mb ou 10 Mb selon l'environnement de votre réseau. Cette option n'est pas disponible si Négociation automatique est Activée .
Mode duplex	Définit le mode duplex sur intégral ou semi selon l'environnement de votre réseau. Cette option n'est pas disponible si Négociation automatique est Activée .

Tableau 4-2. Paramètres LAN IPMI

Paramètre	Description
Activer IPMI sur le LAN	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 00000000000000000000.
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 4-3. 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 changements	Enregistre les modifications apportées à la configuration du réseau. REMARQUE : Les changements appliqués aux paramètres d'adresse IP 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. Tous les autres changements nécessitent la réinitialisation du NIC, qui peut provoquer une perte brève de connectivité.

Configuration des paramètres de sécurité réseau

 **REMARQUE :** Vous devez avoir le droit de **configurer le DRAC 5** pour effectuer les étapes suivantes.

1. Dans l'arborescence **Système**, cliquez sur **Accès à distance**.
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 et cliquez sur **Appliquer les changements**.

Le [tableau 4-4](#) décrit les paramètres de la page **Sécurité réseau**.

5. Cliquez sur le bouton approprié de la page **Sécurité réseau** pour continuer. Consultez le [tableau 4-5](#).

Tableau 4-4. 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 autorisée.
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 d'adresse 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 d'adresse IP	Configure 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 d'adresse IP	Détermine la période en secondes pendant laquelle doivent se produire des échecs du nombre de défaillances du bloc IP pour déclencher la période de pénalité du bloc IP.
Période de pénalité avant blocage d'adresse 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 4-5. Boutons de la page Sécurité réseau

Bouton	Description
Imprimer	Imprime la page Sécurité réseau
Actualiser	Recharge la page Sécurité réseau
Appliquer les changements	Enregistre les modifications apportées à la page Sécurité réseau .
Retour à la page Configuration réseau	Retourne à la page Configuration réseau .

Ajout et configuration des utilisateurs DRAC 5

Pour gérer votre système avec le DRAC 5 et maintenir la sécurité du système, créez des utilisateurs et octroyez-leur des droits d'administration spécifiques (*autorisation basée sur les rôles*). Pour une sécurité accrue, vous pouvez aussi configurer des alertes qui sont envoyées par e-mail à des utilisateurs spécifiques lorsqu'un événement système spécifique se produit.

Pour ajouter et configurer des utilisateurs DRAC 5, effectuez les étapes suivantes :

 **REMARQUE :** Vous devez avoir le droit de configurer le DRAC 5 pour effectuer les étapes suivantes.

1. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Utilisateurs**.

La page **Utilisateurs** apparaît et inclut l'état, le **privilege RAC**, le **privilege LAN IPMI** et le **privilege série IPMI** de chaque utilisateur.

3. Dans la colonne **ID d'utilisateur**, cliquez sur un ID d'utilisateur.

4. Sur la page **Configuration utilisateur**, configurez les propriétés et les privilèges de l'utilisateur.

Le [tableau 4-6](#) décrit les **Paramètres généraux** pour configurer un nom d'utilisateur et un mot de passe DRAC (nouveau ou existant).

Le [tableau 4-7](#) décrit les **Privilèges d'utilisateur IPMI** pour configurer les privilèges LAN de l'utilisateur.

Le [tableau 4-8](#) décrit les Droits de groupe d'utilisateurs pour les paramètres **Privilèges d'utilisateur IPMI** et **Privilèges d'utilisateur DRAC**.

Le [tableau 4-9](#) décrit les droits du Groupe DRAC. Si vous ajoutez un privilège d'utilisateur DRAC à Administrateur, Utilisateur privilégié ou Invité, le Groupe DRAC bascule sur le groupe **Personnalisé**.

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

6. Cliquez sur le bouton approprié de la page **Configuration utilisateur** pour continuer. Consultez le [tableau 4-10](#).

Tableau 4-6. 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 avec 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 comporter les caractères / (barre oblique) ou . (point). REMARQUE : Si le nom d'utilisateur est modifié, le nouveau nom n'apparaîtra 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 Confirmez 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 DRAC 5.
Confirmez le nouveau mot de passe	Vous devez saisir de nouveau le mot de passe de l'utilisateur du DRAC 5 pour le confirmer.

Tableau 4-7. Privilèges d'utilisateur IPMI

Propriété	Description
Maximum de privilèges utilisateur accordés sur le LAN	Spécifie le privilège maximum de l'utilisateur sur le canal LAN IPMI sur un des groupes d'utilisateurs suivants : Administrateur , Opérateur , Utilisateur ou Aucun .
Maximum de privilèges utilisateur accordés sur le port série	Spécifie le privilège maximum de l'utilisateur sur le canal série IPMI sur l'une des options suivantes : Administrateur , Opérateur , Utilisateur ou Aucun .
Activation des communications série sur le LAN	Permet à l'utilisateur d'utiliser les communications série IPMI sur le LAN. Lorsque cette option est sélectionnée, ce privilège est activé.

Tableau 4-8. Privilèges d'utilisateur DRAC

Propriété	Description
Groupe DRAC	Spécifie le privilège maximum de l'utilisateur DRAC sur l'une des options suivantes : Administrateur , Utilisateur privilégié , Invité , Aucun ou Personnalisé . Consultez le tableau 4-9 pour les droits du Groupe DRAC .
Ouvrir une session DRAC	Permet à l'utilisateur d'ouvrir une session DRAC.
Configurer le DRAC	Permet à l'utilisateur de configurer le DRAC.
Configuration des 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.
Exécution des commandes de contrôle du serveur	Permet à l'utilisateur d'exécuter des commandes racadm.
Accès à la redirection de console	Permet à l'utilisateur d'exécuter le redirection de console.
Accès 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 d'essai (e-mail et PET) à un utilisateur spécifique.
Exécution des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Tableau 4-9. Droits de groupe DRAC

Groupe d'utilisateurs	Droits accordés
Administrateur	Ouvrir une session DRAC, Configurer le DRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des 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 DRAC, Effacer les journaux, Exécuter des commandes de contrôle du serveur , Accéder à la redirection de console , Accéder au média virtuel , Tester les alertes.
Invité	Ouvrir une session DRAC.
Personnalisé	Sélectionne parmi les autorisations suivantes : Ouvrir une session DRAC, Configurer le DRAC, Configurer des 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 4-10. Boutons de la page Configuration utilisateur

--	--

Bouton	Action
Imprimer	Imprime la page Configuration utilisateur
Actualiser	Recharge la page Configuration utilisateur
Retour à la page Utilisateurs	Retourne à la page Utilisateurs .
Appliquer les changements	Enregistre les modifications apportées à la configuration du réseau.

Configuration et gestion de certificats Active Directory (schémas standard et étendu)

 **REMARQUE** : Vous devez avoir le droit de **Configurer le DRAC 5** pour configurer Active Directory et télécharger et afficher un certificat Active Directory.

 **REMARQUE** : Pour plus d'informations sur la configuration d'Active Directory et sur la manière de configurer Active Directory avec le schéma standard ou étendu, consultez la section « [Utilisation du DRAC 5 avec Microsoft Active Directory](#) ».

Utilisez le service Microsoft® Active Directory® pour configurer votre logiciel afin de fournir l'accès au DRAC 5. Le service vous permet d'ajouter et de contrôler les droits d'utilisateur DRAC 5 de vos utilisateurs existants.

Consultez la section « [Utilisation du DRAC 5 avec Microsoft Active Directory](#) » pour plus d'informations.

Pour accéder au menu principal d'Active Directory :

1. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Active Directory**.

Le [tableau 4-11](#) énumère les options de la page **Menu principal d'Active Directory**. Les boutons répertoriés dans le [tableau 4-12](#) sont disponibles sur la page **Menu principal d'Active Directory**.

Tableau 4-11. Options de la page Menu principal d'Active Directory

Champ	Description
Configurer Active Directory	Configure les paramètres du nom DRAC d'Active Directory, du nom de domaine racine, du nom de domaine DRAC, du délai d'attente de l'authentification Active Directory, de la sélection du schéma d'Active Directory et du groupe de rôles.
Exporter le certificat d'autorité de certification 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 d'autorité de certification d'Active Directory	Affiche le certificat Active Directory qui a été téléchargé sur le DRAC.

Tableau 4-12. Boutons de la page Menu principal d'Active Directory

Bouton	Définition
Imprimer	Imprime le contenu de la fenêtre ouverte sur l'imprimante par défaut
Suivant	Accède à la page d'option suivante sélectionnée.

Configuration d'Active Directory (schémas standard et 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**, entrez les paramètres d'Active Directory.

Le [tableau 4-13](#) 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. Consultez le [tableau 4-14](#).

5. Pour configurer les groupes de rôles pour le schéma standard d'Active Directory, cliquez sur un groupe de rôles particulier (1-5). Voir [tableau 4-15](#) et [tableau 4-16](#).

 **REMARQUE** : Pour enregistrer les paramètres de la page **Configuration et gestion d'Active Directory**, vous devez cliquer sur **Appliquer** avant de passer à la page **Groupe de rôles personnalisé**.

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

Paramètre	Description
Activer Active Directory	Active Active Directory. Sélectionné = Activé ; Désélectionné = Désactivé.
Nom de domaine racine	Nom de domaine racine d'Active Directory. Cette valeur est nulle 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 DRAC	Nom qui identifie de façon unique la carte DRAC 5 dans Active Directory. Cette valeur est nulle par défaut. Le nom doit être une chaîne de 1 à 254 caractères ASCII, sans espace entre les caractères.
Nom de domaine DRAC	Nom DNS (chaîne de caractères) du domaine où l'objet Active Directory du DRAC 5 réside. Cette valeur est nulle 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 changer les paramètres d'un groupe de rôles, cliquez sur son numéro 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 de la page Configuration et gestion d'Active Directory, vous perdrez tous les paramètres.
Nom du groupe	Nom qui identifie le groupe de rôles dans la version d'Active Directory associée à la carte DRAC 5.
Domaine du groupe	Domaine auquel appartient le groupe.
Privilège du groupe	Niveau de privilège du groupe.

Tableau 4-14. 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 changements apportés à la page Configuration et gestion d'Active Directory.
Retour à la page Menu principal d'Active Directory	Retourne à la page Menu principal d'Active Directory.

Tableau 4-15. Privilèges de groupes de rôles

Paramètre	Description
Niveau de privilèges du groupe de rôles	Spécifie le privilège maximum de l'utilisateur DRAC sur l'une des options suivantes : Administrateur, Utilisateur privilégié, Invité, Aucun ou Personnalisé. Consultez le tableau 4-16 pour les droits possibles pour les groupes de rôles .
Ouvrir une session DRAC	Permet à l'utilisateur d'ouvrir une session DRAC.
Configurer le DRAC	Permet à l'utilisateur de configurer le DRAC.
Configuration des 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.
Exécution des commandes de contrôle du serveur	Permet à l'utilisateur d'exécuter des commandes racadm.
Accès à la redirection de console	Permet à l'utilisateur d'exécuter la redirection de console.
Accès 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 d'essai (e-mail et PET) à un utilisateur spécifique.
Exécution des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Tableau 4-16. Droits des groupes de rôles

Propriété	Description
-----------	-------------

Administrateur	Ouvrir une session DRAC, Configurer le DRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des 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 DRAC, Effacer les journaux, Exécuter des commandes de contrôle du serveur, Accéder à la redirection de console, Accéder au média virtuel , Tester les alertes.
Invité	Ouvrir une session DRAC
Personnalisé	Sélectionne parmi les autorisations suivantes : Ouvrir une session DRAC, Configurer le DRAC, Configurer des 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

Exportation d'un certificat d'autorité de certification d'Active Directory

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Exporter le certificat d'autorité de certification 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 d'accès au fichier relatif au certificat que vous téléchargez. Vous devez taper le chemin de fichier absolu qui inclut le chemin complet et le nom de fichier complet, y compris l'extension du fichier.
3. Cliquez sur **Appliquer**.
 4. Cliquez sur le bouton approprié de la page **Téléchargement d'un certificat** pour continuer. Consultez le [tableau 4-17](#).

Tableau 4-17. Boutons de la page **Téléchargement d'un certificat**

Bouton	Description
Imprimer	Imprime la page Téléchargement d'un certificat .
Retour à la page Menu principal d'Active Directory	Retourne à la page Menu principal d'Active Directory .
Appliquer	Applique le certificat au micrologiciel DRAC 5.

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 d'autorité de certification Active Directory

Utilisez la page **Menu principal d'Active Directory** pour afficher un certificat de serveur d'autorité de certification pour votre DRAC 5.

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Afficher le certificat d'autorité de certification d'Active Directory** et cliquez sur **Suivant**.
Le [tableau 4-18](#) décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.
Le [tableau 4-19](#) décrit les boutons disponibles sur la page **Afficher le certificat d'autorité de certification d'Active Directory**.
2. Cliquez sur le bouton approprié de la page **Afficher le certificat d'autorité de certification d'Active Directory** pour continuer. Voir [tableau 4-19](#).

Tableau 4-18. Informations relatives au certificat d'autorité de certification d'Active Directory

Champ	Description
Numéro de série	Numéro de série du certificat.
Informations sur le sujet	Attributs du certificat entrés par le demandeur.
Informations sur l'émetteur	Attributs du certificat renvoyés par l'émetteur.
Valide du	Date d'émission du certificat.
Valide jusqu'au	Date d'expiration du certificat.

Tableau 4-19. Boutons de la page **Afficher le certificat d'autorité de certification d'Active Directory**

Bouton	Description
Imprimer	Imprime le certificat d'autorité de certification d'Active Directory .
Retour à la page Menu principal d'Active Directory	Retourne à la page Menu principal d'Active Directory.

Sécurisation des communications 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 :

- 1 Protocole Secure Sockets Layer (SSL)
- 1 Requête de signature de certificat (CSR)
- 1 Accès au menu principal SSL
- 1 Génération d'une nouvelle CSR
- 1 Téléchargement d'un certificat du serveur
- 1 Affichage d'un certificat du serveur

Protocole 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 clé privée, SSL est une technique répandue permettant la communication authentifiée et cryptée entre les clients et les serveurs afin d'empêcher toute écoute indiscreète dans un réseau.

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

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

Ce processus de cryptage fournit un haut niveau de protection de données. 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 pour un certificat de serveur sécurisé. Les certificats de serveur sécurisé garantissent l'identité d'un système distant et assurent que les informations échangées avec le système distant ne peuvent être ni affichées, ni modifiées par d'autres. Pour sécuriser votre DRAC, nous vous conseillons vivement de générer une CSR, de l'envoyer à une autorité de certification et de télécharger le certificat qu'elle vous envoie.

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

Une fois que l'autorité de certification approuve la CSR et vous envoie le certificat, vous devez le télécharger dans le micrologiciel DRAC. Les informations de CSR stockées dans le micrologiciel DRAC doivent correspondre aux informations du certificat.

Accès au menu principal SSL

1. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **SSL**.

Utilisez les options de la page **Menu principal SSL** (voir [tableau 4-20](#)) pour générer une CSR à envoyer à une autorité de certification. Les informations de la CSR sont enregistrées dans le micrologiciel DRAC 5. Les boutons répertoriés au [tableau 4-21](#) sont disponibles sur la page **Menu principal SSL**.

Tableau 4-20. 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 et pouvoir générer une CSR à envoyer à une autorité de certification pour demander un certificat de Web sécurisé. AVIS : La nouvelle CSR remplace toujours la CSR présente sur le micrologiciel. Pour qu'une autorité de certification accepte votre CSR, la CSR du micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification.
Télécharger le certificat du 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. AVIS : 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 du serveur	Cliquez sur Suivant pour afficher un certificat de serveur existant.

Tableau 4-21. Boutons du menu principal SSL

Bouton	Description
Imprimer	Imprime la page Menu principal SSL .
Suivant	Accède à la page suivante.

Génération d'une nouvelle requête de signature de certificat

 **REMARQUE :** La nouvelle CSR remplace toujours la CSR présente sur le micrologiciel. Pour qu'une autorité de certification accepte votre CSR, la CSR du micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification. 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.
Le [tableau 4-22](#) décrit les options de la page **Générer une requête de signature de certificat (CSR)**.
3. Cliquez sur **Générer** enregistrer ou afficher la CSR.
4. Cliquez sur le bouton approprié de la page **Générer une requête de signature de certificat (CSR)** pour continuer. Voir [tableau 4-23](#).

Tableau 4-22. Options de la page **Générer une requête de signature de certificat (CSR)**

Champ	Description
Nom de domaine	Nom exact à certifier (normalement, le nom de domaine du serveur Web comme, par exemple, www.compagnieux.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 compagnie	Nom associé à cette compagnie (par exemple, Compagnie XYZ). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Service de la compagnie	Nom associé au service, 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	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 du département	Département ou 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 de pays	Nom du pays où se trouve l'entité qui fait la demande de certification. Utilisez le menu déroulant pour sélectionner le pays.
E-mail	Adresse e-mail associée à la CSR. Vous pouvez taper l'adresse électronique de votre société ou une adresse électronique que vous voulez associer à la CSR. Ce champ est optionnel.

Tableau 4-23. 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 à la page Menu principal SSL	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 du 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 d'accès au fichier relatif au certificat que vous téléchargez. Vous devez taper le chemin de fichier absolu qui inclut le chemin complet et le nom de fichier complet, y compris l'extension du fichier.

3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié de la page pour continuer. Consultez le [tableau 4-24](#).

Tableau 4-24. Boutons de la page **Téléchargement d'un certificat**

Bouton	Description
Imprimer	Imprime la page Téléchargement d'un certificat .
Retour au Menu Principal SSL	Retourne à la page Menu principal SSL .
Appliquer	Applique le certificat au micrologiciel DRAC 5.

Affichage d'un certificat du serveur

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

Le [tableau 4-25](#) décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

2. Cliquez sur le bouton approprié de la page **Afficher le certificat du serveur** pour continuer. Voir [tableau 4-26](#).

Tableau 4-25. Informations relatives au certificat

Champ	Description
Numéro de série	Numéro de série du certificat
Informations sur le sujet	Attribut du certificat entrés par le demandeur
Informations sur l'émetteur	Attributs du certificat renvoyés par l'émetteur
Valide du	Date d'émission du certificat
Valide jusqu'au	Date d'expiration du certificat

Tableau 4-26. Boutons de la page **Afficher le certificat du serveur**

Bouton	Description
Imprimer	Imprime la page Afficher le certificat du serveur .
Retour au Menu Principal SSL	Retourne à la page Menu principal SSL .

Configuration des modes série et terminal

Configuration du mode série IPMI et RAC

1. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Série**.
3. Configurez les paramètres série IPMI.

Le [tableau 4-27](#) donne des informations sur les paramètres série IPMI.

4. Configurez les paramètres série RAC.

Le [tableau 4-28](#) donne des informations sur les paramètres série RAC.

5. Cliquez sur **Appliquer les changements**.

6. Cliquez sur le bouton approprié de la page **Configuration série** pour continuer. Consultez le [tableau 4-29](#).

Tableau 4-27. Paramètres série IPMI

Paramètre	Description
Paramètre du mode de connexion	<ul style="list-style-type: none"> 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 débit	<ul style="list-style-type: none"> Aucun : contrôle du débit matériel désactivé RTS/CTS : contrôle du débit matériel activé
Limite du niveau de privilège du canal	<ul style="list-style-type: none"> Administrateur Opérateur Utilisateur

Tableau 4-28. Paramètres série RAC

Paramètre	Description
Activé	Active ou désactive la console série RAC. Sélectionné = Activé ; Désélectionné = Désactivé
Nombre maximal de sessions	Nombre maximum 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 1920 secondes. La valeur par défaut est 300 secondes. Utilisez 0 seconde pour désactiver la fonctionnalité de délai d'attente.
Redirection activée	Active ou désactive la redirection de console. Sélectionné = Activé ; Désélectionné = 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 de l'historique de la zone tampon	Taille de l'historique série de la zone tampon, 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 DRAC à exécuter lors d'une ouverture de session valide.

Tableau 4-29. Paramètres de la page Configuration en série

Bouton	Description
Imprimer	Imprime la page Configuration en série .
Actualiser	Actualise la page Configuration en série .
Appliquer les changements	Applique les changements série IPMI et RAC.
Paramètres du mode terminal	Ouvre la page Paramètres du mode terminal .

Configuration du mode terminal

1. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Série**.
3. Sur la page **Configuration en série**, cliquez sur **Paramètres du mode terminal**.
4. Configurez les paramètres du mode terminal.

Le [tableau 4-30](#) donne des informations sur les paramètres du mode terminal.

5. Cliquez sur **Appliquer les changements**.
6. Cliquez sur le bouton approprié de la page **Paramètres du mode terminal** pour continuer. Voir [tableau 4-31](#).

Tableau 4-30. 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 : <ul style="list-style-type: none"> 1 Le BMC génère un caractère <retour><espace><retour> lorsque <retour> ou <suppr> est reçu 1 Le BMC génère un caractère <suppr> lorsque <retour> 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 <NUL>.

Tableau 4-31. 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 changements	Applique les changements des paramètres du mode terminal.

Configuration des communications série sur le LAN

 **REMARQUE :** Pour plus d'informations sur les Communications série sur le LAN, consultez le *Guide d'utilisation du contrôleur de gestion de la carte mère de Dell OpenManage*.

1. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Communications série sur le LAN**.
3. Configurez les paramètres de communications série sur le LAN.
Le [tableau 4-32](#) fournit des informations sur les paramètres de la page **Configuration des communications série sur le LAN**.
4. Cliquez sur **Appliquer les changements**.
5. Configurez les paramètres avancés, si nécessaire. Sinon, cliquez sur le bouton approprié de la page **Configuration des communications série sur le LAN** pour continuer (voir [tableau 4-33](#)).

Pour configurer les paramètres avancés, effectuez les étapes suivantes :

- a. Cliquez sur **Paramètres avancés**.
- b. Sur la page **Paramètres avancés de la configuration des communications série sur le LAN**, configurez les paramètres avancés, si nécessaire. Voir [tableau 4-34](#).
- c. Cliquez sur **Appliquer les changements**.
- d. Cliquez sur le bouton approprié de la page **Paramètres avancés de la configuration des communications série sur le LAN** pour continuer. Voir [tableau 4-35](#).

Tableau 4-32. Paramètres de la page Configuration des communications série sur le LAN

Paramètre	Description
Activation des communications série sur le LAN	Active les communications série sur le LAN. Sélectionné = Activé ; Désélectionné = Désactivé.
Débit en bauds	Vitesse de transmission des données IPMI. Sélectionnez 9 600 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 des communications série IPMI sur le LAN : Administrateur , Opérateur ou Utilisateur .

Tableau 4-33. Boutons de la page Configuration des communications série sur le LAN

Bouton	Description
Imprimer	Imprime la page Configuration des communications série sur le LAN .
Actualiser	Actualise la page Configuration des communications série sur le LAN .
Paramètres avancés	Ouvre la page Paramètres avancés de la configuration des communications série sur le LAN .
Appliquer les changements	Applique les paramètres de la page Configuration des communications série sur le LAN .

Tableau 4-34. Paramètres de la page Paramètres avancés de la configuration des communications série sur le 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.
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 4-35. Boutons de la page Paramètres avancés de la configuration des communications série sur le LAN

Bouton	Description
Imprimer	Imprime la page Paramètres avancés de la configuration des communications série sur le LAN .
Actualiser	Actualise la page Paramètres avancés de la configuration des communications série sur le LAN .
Retour à la page Configuration des communications série sur le LAN	Retourne à la page Configuration des communications série sur le LAN .
Appliquer les changements	Applique les paramètres de la page Paramètres avancés de la configuration des communications série sur le LAN .

Configuration des services

 **REMARQUE :** Pour modifier ces paramètres, vous devez avoir le droit de **configurer le DRAC 5**. De plus, l'utilitaire de ligne de commande RACADM distant peut seulement être activé si l'utilisateur est enregistré en tant que root.

- Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
- Cliquez sur l'onglet **Configuration**, puis sur **Services**.
- Configurez les services suivants, si nécessaire :
 - Web Server ([Tableau 4-36](#))
 - SSH ([Tableau 4-37](#))
 - Telnet ([Tableau 4-38](#))
 - RACADM distant ([Tableau 4-39](#))
 - Agent SNMP ([Tableau 4-40](#))
 - Agent de récupération automatique du système ([Tableau 4-41](#))

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.

- Cliquez sur **Appliquer les changements**.
- Cliquez sur le bouton approprié de la page **Services** pour continuer. Voir [tableau 4-42](#).

Tableau 4-36. Paramètres de Web Server

Paramètre	Description
Activé	Active ou désactive Web Server. Sélectionné = Activé ; Désélectionné = Désactivé.

Nombre maximal de sessions	Nombre maximum de sessions simultanées autorisées pour ce système.
Sessions actives	Nombre de sessions actuelles sur le système, inférieur ou égal à 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'attente est atteint. Les changements apportés au paramètre de délai d'attente n'affectent pas la session actuelle. Lorsque vous modifiez le paramètre de délai d'attente, vous devez fermer puis ouvrir une session pour appliquer le nouveau paramètre. La plage du délai d'attente est comprise entre 60 et 1920 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 4-37. Paramètres SSH

Paramètre	Description
Activé	Active ou désactive SSH. Sélectionné = Activé ; Désélectionné = Désactivé.
Nombre maximal de sessions	Nombre maximum 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 à Nombre maximal de sessions .
Délai d'attente	Délai d'attente Secure Shell en secondes. Plage = 60 à 1920 secondes. Entrez 0 seconde pour désactiver le fonctionnalité de délai d'attente. 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 4-38. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Sélectionné = Activé ; Désélectionné = Désactivé.
Nombre maximal de sessions	Nombre maximum 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 à Nombre maximal de sessions .
Délai d'attente	Délai d'attente Secure Shell en secondes. Plage = 60 à 1920 secondes. Entrez 0 seconde pour désactiver le fonctionnalité de délai d'attente. 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 4-39. Paramètres RACADM distant

Paramètre	Description
Activé	Active ou désactive RACADM distant. Sélectionné = Activé ; Désélectionné = Désactivé.
Nombre maximal de sessions	Nombre maximum 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 à Nombre maximal de sessions .

Tableau 4-40. Paramètres d'agent SNMP

Paramètre	Description
Activé	Active ou désactive l'agent SNMP. Sélectionné = Activé ; Désélectionné = 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 4-41. Paramètre de l'agent de récupération automatique du système

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

Tableau 4-42. Boutons de la page Services

Bouton	Description
Imprimer	Imprime la page Services .
Actualiser	Actualise la page Services .

Questions les plus fréquentes

Le [tableau 4-43](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 4-43. Gestion et récupération d'un système distant : Questions les plus fréquentes

Question	Réponse
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.	<p>Le DRAC 5 est doté d'un certificat de serveur DRAC 5 par défaut qui assure la sécurisation du réseau pour l'interface Web et les fonctionnalités racadm à distance. 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).</p> <p>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 de domaine (CN) de la CSR corresponde à l'adresse IP du DRAC 5 (192.168.0.120, par exemple) ou au nom DRAC DNS enregistré.</p> <p>Pour garantir que la CSR correspond au nom DRAC DNS enregistré, effectuez les étapes suivantes :</p> <ol style="list-style-type: none"> 1. Dans l'arborescence Système, cliquez sur Accès à distance. 2. Cliquez sur l'onglet Configuration, puis sur Réseau. 3. Sur la page Paramètres réseau, effectuez les étapes suivantes : <ol style="list-style-type: none"> a. Cochez la case Enregistrer le DRAC auprès du DNS. b. Dans le champ Nom DRAC DNS, entrez le nom DRAC. 4. Cliquez sur Appliquer les changements. <p>Consultez la section « Sécurisation des communications DRAC 5 via SSL et des certificats numériques » pour plus d'informations sur la génération de CSR et l'émission de certificats.</p>
L'utilitaire racadm à distance et les services Web ne sont plus disponibles lorsqu'on change les propriétés. Pourquoi ?	<p>Lorsque vous réinitialisez le Web Server d'un DRAC 5, il peut s'écouler une minute avant que les services RACADM à distance et l'interface Web ne redeviennent disponibles.</p> <p>Le Web Server du DRAC 5 Web est réinitialisé dans les cas suivants :</p> <ul style="list-style-type: none"> 1 Quand la configuration réseau ou les propriétés de sécurité réseau sont modifiées à l'aide de l'interface utilisateur Web DRAC 5 1 Quand la propriété <code>cfgRacTuneHttpsPort</code> est modifiée (y compris lorsqu'une commande <code>config -f <fichier config></code> la modifie) 1 Quand on utilise <code>racresetcfg</code> 1 Quand le DRAC 5 est réinitialisé 1 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 qui n'est pas fiable.	Le DRAC 5 est doté d'un certificat de serveur DRAC 5 par défaut qui assure la sécurisation du réseau pour l'interface Web et les fonctionnalités racadm à distance. Ce certificat n'a pas été émis par une autorité de certification de confiance. Pour résoudre ce problème de sécurité, téléchargez un certificat de serveur DRAC 5 émis par une autorité de certification de confiance (Thawte ou Verisign, par exemple). Consultez la section « Sécurisation des communications DRAC 5 via SSL et des certificats numériques » pour plus d'informations sur l'émission de certificats.
Le message suivant s'affiche pour des raisons inconnues : Remote Access: SNMP Authentication Failure (Accès à distance : Échec d'authentification SNMP) Pourquoi ?	<p>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 est « public » et le nom de communauté Set est « 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 ».</p> <p>Vous pouvez changer le nom de communauté du DRAC 5 avec RACADM.</p> <p>Pour afficher le nom de communauté du DRAC 5, utilisez la commande suivante :</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>Pour définir le nom de communauté du DRAC 5, utilisez la commande suivante :</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nom de communauté></pre> <p>Pour ne pas générer d'interruption d'authentification SNMP, vous devez entrer des noms de communauté qui seront acceptés par l'agent. Comme le DRAC 5 n'accepte qu'un seul nom de communauté, vous devez entrer le même nom pour les communautés Get et Set lorsque vous configurez les découvertes sous IT Assistant.</p>

[Retour à la page du sommaire](#)

Récupération et dépannage du système géré

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Premières étapes de dépannage d'un système distant](#)
- [Gestion de l'alimentation d'un système distant](#)
- [Affichage des informations sur le système](#)
- [Utilisation du journal des événements système \(SEL\)](#)
- [Affichage de l'écran de la dernière panne système](#)
- [Utilisation du journal du RAC](#)
- [Utilisation de la console de diagnostics](#)
- [Dépannage des problèmes de réseau](#)
- [Dépannage des problèmes d'alerte](#)

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 s'est bloqué. Pour plus d'informations sur le dépannage de votre DRAC 5, consultez la section « [Déploiement de votre système d'exploitation via VM-CLI](#) ».

- 1 Dépannage d'un système distant
- 1 Gestion de l'alimentation d'un système distant
- 1 Utilisation du journal des événements système (SEL)
- 1 Affichage de l'écran de la dernière panne système
- 1 Utilisation du journal du RAC
- 1 Utilisation de la console de diagnostics

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 subitement en panne ou seulement bloqué ?
3. S'il est hors tension, est-ce que l'alimentation a été coupée soudainement ?

Si le système est en panne, vérifiez l'écran de la dernière panne (consultez la section « [Affichage de l'écran de la dernière panne système](#) ») et utilisez la redirection de console (« [Fréquences d'actualisation des résolutions d'écran prises en charge sur le système géré](#) ») et la gestion d'alimentation à distance (consultez la section « [Gestion de l'alimentation d'un système distant](#) ») pour redémarrer le système et surveiller la procédure 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 :

- 1 Effectuer un arrêt normal via le système d'exploitation lors du redémarrage, et mettre sous tension puis hors tension le système.
- 1 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 d'**exécuter les commandes d'action du serveur** pour effectuer les actions de gestion de l'alimentation.

Sélection des actions de contrôle de l'alimentation

1. Sélectionnez l'une des **actions de contrôle de l'alimentation** suivantes.
 - 1 **Allumer le système** : met le système sous tension (équivalent à appuyer sur le bouton marche/arrêt quand le système est hors tension).
 - 1 **Arrêter le système** : met le système hors tension (équivalent à appuyer sur le bouton marche/arrêt quand le système est sous tension).
 - 1 **Réinitialiser le système** : réinitialise le système (équivalent à appuyer sur le bouton de réinitialisation) ; l'alimentation n'est pas coupée si vous utilisez cette fonction.
 - 1 **Exécuter un cycle d'alimentation sur le système** : mise hors tension, puis redémarrage (à froid) du 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 5-1](#)).

Tableau 5-1. **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

Affichage des informations sur le système

La page **Résumé du système** affiche des informations sur les composants système suivants :

- 1 Châssis principal du système
- 1 Remote Access Controller
- 1 Contrôleur de gestion de la carte mère

Pour accéder aux informations système, développez l'arborescence **Système** et cliquez sur **Propriétés**.

Châssis principal du système

Le [tableau 5-2](#) et le [tableau 5-3](#) décrivent les propriétés du châssis principal du système.

 **REMARQUE :** Pour recevoir les informations sur le **nom d'hôte** et le **nom du système d'exploitation**, les services DRAC 5 doivent être installés sur le système géré.

Tableau 5-2. **Champs d'Informations sur le 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 5-3. **Champs de 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

Le [tableau 5-4](#) décrit les propriétés du Remote Access Controller.

Tableau 5-4. **Champs d'informations sur le RAC**

Champ	Description
Nom	Nom abrégé.
Informations sur le produit	Nom complet.
Version du matériel	Version de carte RAC ou « inconnue ».
Version du micrologiciel	Niveau de version de micrologiciel actuel du DRAC 5.
Mise à jour de 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

Le [tableau 5-5](#) décrit les propriétés du contrôleur de gestion de la carte mère (BMC).

Tableau 5-5. Champs d'informations sur le contrôleur BMC

Champ	Description
Nom	« Contrôleur de gestion de la carte mère ».
Version IPMI	Version d'interface de gestion de plateforme intelligente (IPMI).
Nombre de sessions actives possibles	Nombre maximum de sessions qui peuvent être actives en même temps.
Nombre de sessions actives	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, effectuez les étapes suivantes :

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 au [tableau 5-6](#).

3. Cliquez sur le bouton approprié de la page **Journal des événements système** pour continuer (voir [Tableau 5-7](#)).

Tableau 5-6. Icônes indicatrices de condition

Icône/Catégorie	Description
	Une marque 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 (panne).
	Une icône représentant un point d'interrogation indique que la condition est inconnue.
Date et 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, et basé sur une horloge de 24 heures.
Description	Une brève description de l'événement

Tableau 5-7. 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 de l'autorisation d'effacer le journal.
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 la dernière version de 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.

Affichage de l'écran de la dernière panne système

➔ **AVIS** : 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 le plus récent, qui comprend des informations sur les événements qui se sont produits avant la panne du système. Les informations sur la dernière panne du système sont enregistrées dans la mémoire du DRAC 5 et sont accessibles à distance.

Pour afficher la page **Écran de la dernière panne**, effectuez les étapes suivantes :

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 le [tableau 5-8](#)) en haut à droite de l'écran :

Tableau 5-8. 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 s'assurer que la fonctionnalité **Écran de la dernière panne** fonctionne correctement. Consultez la section « [Configuration du système géré pour capturer l'écran de la dernière panne](#) » pour obtenir des informations supplémentaires.

Utilisation du journal du RAC

Le **Journal du RAC** est un journal permanent conservé dans le micrologiciel DRAC 5. Le journal contient une liste des actions d'utilisateur (ouverture, fermeture de sessions et modifications des règles de sécurité par exemple) et des alertes envoyées par le DRAC 5. Les entrées les plus anciennes sont effacées quand le journal est plein.

Pour accéder au journal du RAC, effectuez les étapes suivantes :

1. Dans l'arborescence **Système**, cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Journal du RAC**.

Le **Journal du RAC** fournit les informations répertoriées au [tableau 5-9](#).

Tableau 5-9. Informations sur la page du journal du RAC

Champ	Description
Date et heure	Date et heure en anglais (par exemple, Dec 19 16:55:47). Si le DRAC 5 ne peut pas communiquer avec le système géré lors de son premier démarrage, l'heure affichée est celle du démarrage du système.
Source	Interface qui a provoqué l'événement.
Description	Description brève de l'événement et nom d'utilisateur qui s'est connecté au DRAC 5.

Utilisation des boutons de la page Journal du RAC

La page **Journal du RAC** dispose des boutons suivants (consultez le [tableau 5-10](#)).

Tableau 5-10. Boutons du journal du RAC

Bouton	Action
Imprimer	Imprime la page Journal du RAC .
Effacer le journal	Efface les entrées du Journal du RAC .

	REMARQUE : Le bouton Effacer le journal n'apparaît que si vous disposez de l'autorisation d'effacer le journal.
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 la dernière version de 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 console de diagnostics

Le DRAC 5 fournit un ensemble standard d'outils de diagnostic réseau (voir [Tableau 5-11](#)) qui sont 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**, effectuez les étapes suivantes :

1. Dans l'arborescence **Système**, cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Diagnostic**.

Le [tableau 5-11](#) décrit les options disponibles sur la page **Console de diagnostics**. 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 5-11. 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 les informations actuelles 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 de la table de routage utilisée.
gettracelog	Affiche le journal de suivi du DRAC 5. Pour des informations supplémentaires, consultez la section « gettracelog ».

Dépannage des problèmes de réseau

Le journal de suivi interne du DRAC 5 permet aux administrateurs de déboguer les alertes ou la mise en réseau à partir du DRAC 5. Vous pouvez accéder au journal de suivi à partir de l'interface Web du DRAC 5 en cliquant sur l'onglet **Diagnostics**, en tapant la commande **gettracelog** ou la commande **racadm gettracelog**. Pour des informations supplémentaires, consultez la section « [gettracelog](#) ».

Le journal de suivi enregistre les informations suivantes :

- 1 DHCP : fait le suivi des paquets envoyés à un serveur DHCP et reçus de celui-ci.
- 1 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 DRAC 5, c'est-à-dire le micrologiciel DRAC 5 interne, et non pas le système d'exploitation du système géré.

 **REMARQUE :** Le DRAC 5 ne renvoie pas d'ICMP (ping) si le paquet dépasse 1500 octets.

Dépannage des problèmes d'alerte

Utilisez les informations d'interruptions SNMP journalisées pour dépanner un type particulier d'alerte DRAC 5. Les livraisons d'interruptions SNMP sont journalisées dans le journal de suivi par défaut. Cependant, comme SNMP ne confirme pas la livraison des interruptions, utilisez un analyseur de réseau ou un outil tel que **snmputil** de Microsoft pour effectuer le suivi des paquets sur le système géré.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation du DRAC 5 avec Microsoft Active Directory

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Avantages et inconvénients des schémas étendu et standard](#)
- [Présentation du schéma étendu d'Active Directory](#)
- [Présentation du schéma standard d'Active Directory](#)
- [Activation de SSL sur un contrôleur de domaine](#)
- [Utilisation d'Active Directory pour ouvrir une session DRAC 5](#)
- [Questions les plus fréquentes](#)

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 le logiciel de service Microsoft® Active Directory®, il peut être configuré pour vous donner accès au DRAC 5 et vous permettre d'ajouter et de contrôler les privilèges des utilisateurs DRAC 5 pour les utilisateurs présents dans votre logiciel Active Directory.

 **REMARQUE :** L'utilisation d'Active Directory pour reconnaître les utilisateurs DRAC 5 est prise en charge par les systèmes d'exploitation Microsoft Windows® 2000 et Windows Server® 2003.

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur sur le DRAC 5 de deux manières : avec la solution du schéma étendu qui utilise des objets Active Directory définis par Dell ou avec la solution du schéma standard qui n'utilise que des objets des groupes Active Directory.

Avantages et inconvénients des schémas étendu et standard

Lorsque vous utilisez Active Directory pour configurer l'accès au DRAC 5, vous devez choisir soit le schéma étendu soit le schéma standard.

L'utilisation de la solution du schéma étendu a les avantages suivants :

- 1 Tous les objets de contrôle de l'accès sont contenus dans Active Directory.
- 1 La configuration de l'accès utilisateur sur des cartes DRAC 5 avec des niveaux de privilège différents est très flexible.

L'utilisation de la solution du schéma standard a les avantages suivants :

- 1 Aucune extension de schéma n'est nécessaire parce que le schéma standard n'utilise que des objets Active Directory.
- 1 La configuration sur Active Directory est simple.

Présentation du schéma étendu d'Active Directory

Il y a deux manières d'activer le schéma étendu d'Active Directory :

- 1 Avec l'interface utilisateur Web du DRAC 5. Voir « [Configuration du DRAC 5 avec le schéma étendu d'Active Directory et l'interface Web](#) ».
- 1 Avec l'outil CLI RACADM. Voir « [Configuration du DRAC 5 avec le schéma étendu d'Active Directory et RACADM](#) ».

Extensions de schéma d'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 pour répondre aux besoins de leur environnement. Dell a étendu ce schéma pour inclure les modifications nécessaires à la prise en charge de l'authentification et de l'autorisation de la gestion à distance.

Chaque attribut et classe ajouté à un schéma d'Active Directory existant peut être défini par un ID exclusif. Pour que les ID soient uniques dans toute l'industrie, Microsoft maintient une base de données d'identificateurs d'objets (OID) Active Directory de sorte que lorsque des sociétés ajoutent des extensions au schéma, elles sont sûres que ces extensions seront uniques et ne créeront pas de conflits avec d'autres. Pour étendre le schéma de Microsoft Active Directory, Dell a reçu des OID uniques, des extensions de noms uniques et des ID d'attributs uniques liés aux attributs et aux 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 RAC est : 12070 à 12079

La base de données OID d'Active Directory maintenue par Microsoft est disponible à <http://msdn.microsoft.com/certification/ADAcctInfo.asp> en entrant notre extension Dell.

Présentation générale des extensions de schéma de 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, Périphériques et Privilèges. 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 donne aux administrateurs le maximum de flexibilité pour les diverses combinaisons d'utilisateurs, de privilèges de RAC et de périphériques de RAC du réseau sans être pour autant trop compliqué.

Présentation générale des objets d'Active Directory

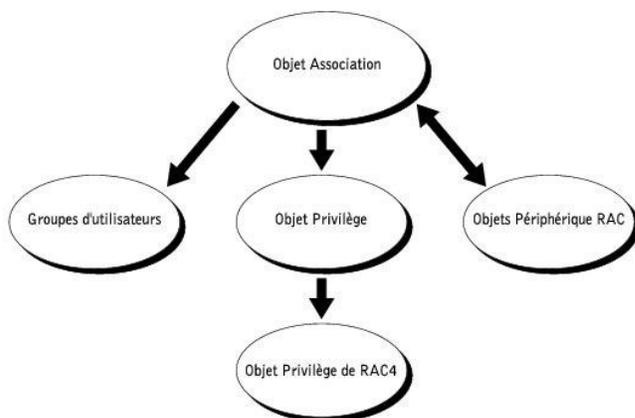
Pour chacun des RAC physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, vous devez créer au moins un objet Association et un objet Périphériques RAC. Vous pouvez créer autant d'objets Association que vous le voulez, et chaque 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 membres de n'importe quel domaine de 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 Périphériques RAC est le lien vers le micrologiciel 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.

La [figure 6-1](#) montre que l'objet Association fournit la connexion nécessaire pour toute les authentifications et autorisations.

Figure 6-1. Configuration typique des objets d'Active Directory



REMARQUE : L'objet Privilège RAC s'applique tant à DRAC 4 qu'à DRAC 5.

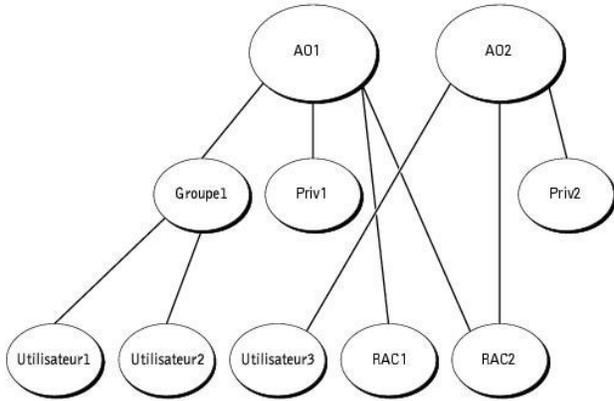
Vous pouvez créer autant d'objets Association que vous le voulez. Cependant, vous devez créer au moins un objet Association, et vous devez avoir un objet Périphérique RAC pour chaque RAC (DRAC 5) du réseau que vous voulez intégrer avec Active Directory pour en gérer l'authentification et l'autorisation.

L'objet Association ne limite pas le nombre d'utilisateurs, de groupes et d'objets Périphérique RAC. Toutefois, l'objet Association ne peut inclure qu'un objet Privilège. 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 (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. La [figure 6-2](#) vous 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 les groupes locaux de domaines et ne fonctionnent pas avec les groupes universels d'autres domaines.

Figure 6-2. Configuration des objets d'Active Directory dans un seul domaine



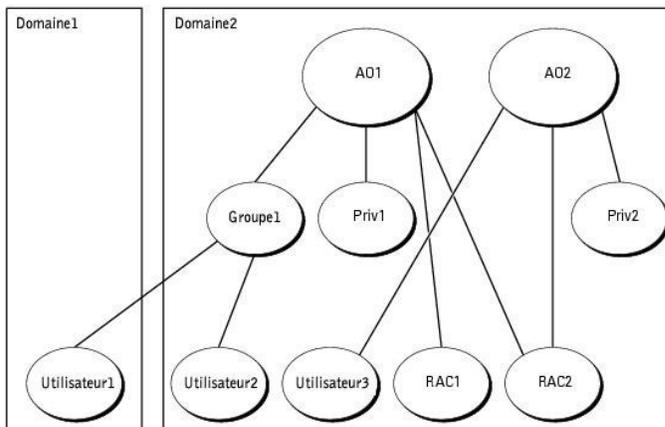
Pour configurer les objets pour le scénario de domaine unique, effectuez les tâches suivantes :

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 Privilèges, Priv1 et Priv2, dans lequel Priv1 a tous les droits (administrateur) et Priv2 a des droits d'ouverture de session.
4. Regroupez Utilisateur1 et Utilisateur2 dans Groupe1.
5. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objets Privilèges dans A01 et RAC1 et RAC2 comme périphériques RAC dans A01.
6. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objets Privilèges dans A02 et RAC2 comme périphériques RAC dans A02.

Consultez la section « [Ajout d'utilisateurs et de privilèges DRAC 5 à Active Directory](#) » pour obtenir des instructions détaillées.

La [figure 6-3](#) fournit un exemple d'objets d'Active Directory dans de multiples domaines. Dans ce scénario, vous avez deux cartes DRAC 5 (RAC1 et RAC2) et trois utilisateurs Active Directory (Utilisateur1, Utilisateur2 et Utilisateur3). Utilisateur1 est dans le Domaine1 ; Utilisateur2 et Utilisateur3 sont dans le Domaine2. Dans ce scénario, configurez Utilisateur1 et Utilisateur2 avec les droits d'administrateur sur les deux cartes DRAC 5 et configurez Utilisateur3 avec les droits d'ouverture de session sur la carte RAC2.

Figure 6-3. Configuration d'objets d'Active Directory dans plusieurs domaines



Pour configurer les objets pour le scénario à plusieurs domaines, effectuez les tâches suivantes :

1. Vérifiez que la fonction de forêt de domaine est en mode natif ou Windows 2003.
2. Créez deux objets Association, A01 (d'étendue Universel) et A02, dans un des domaines.
La [figure 6-3](#) montre les objets dans Domaine2.
3. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux cartes DRAC 5.

4. Créez deux objets Privilèges, Priv1 et Priv2, dans lequel Priv1 a tous les droits (administrateur) et Priv2 a des droits d'ouverture de session.
5. Regroupez Utilisateur1 et Utilisateur2 dans Groupe1. L'étendue du groupe de Groupe1 doit être Universel.
6. Ajoutez Groupe1 comme membre de l'objet Association 1 (AO1), Priv1 comme objets Privilèges 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 Privilèges dans AO2 et RAC2 comme périphériques RAC dans AO2.

Configuration du schéma étendu d'Active Directory 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 d'Active Directory (consultez la section « [Extension du schéma d'Active Directory](#) »).
2. Étendez le snap-in Utilisateurs et ordinateurs Active Directory (consultez la section « [Installation de l'extension de Dell pour le snap-in Utilisateurs et ordinateurs Active Directory](#) »).
3. Ajoutez les utilisateurs DRAC 5 et leurs privilèges à Active Directory (consultez la section « [Ajout d'utilisateurs DRAC 5 et de leurs privilèges à Active Directory](#) »).
4. Activez SSL sur tous vos contrôleurs de domaine (consultez la section « [Activation de SSL sur un contrôleur de domaine](#) »).
5. Configurez les propriétés Active Directory du DRAC 5 en utilisant l'interface Web du DRAC 5 ou RACADM (voir « [Configuration du DRAC 5 avec le schéma étendu d'Active Directory et l'interface Web](#) » ou « [Configuration du DRAC 5 avec le schéma étendu d'Active Directory et RACADM](#) »).

Extension du schéma d'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 privilèges et d'association au schéma Active Directory. Pour étendre le schéma, vous devez avoir des privilèges d'administrateur de schéma pour le propriétaire de rôle FSMO contrôleur de schéma de la forêt de domaine.

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

- 1 Utilitaire Dell Schema Extender
- 1 Fichier script LDIF

Si vous utilisez le fichier script LDIF, l'unité organisationnelle Dell ne sera pas ajoutée au schéma.

Les fichiers LDIF et l'utilitaire Dell Schema Extender se trouvent sur le CD *Dell Systems Management Consoles*, respectivement dans les répertoires suivants :

- 1 *Lecteur de CD:* \support\OMActiveDirectory Tools\RAC4-5\LDIF_Files
- 1 *Lecteur de CD:* \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 afin d'étendre le schéma d'Active Directory, consultez la section « [Utilisation de l'utilitaire Dell Schema Extender](#) ».

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

Utilisation de l'utilitaire Dell Schema Extender

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

1. Dans l'écran d'accueil, cliquez sur **Suivant**.
2. Lisez et saisissez l'avertissement, puis cliquez sur **Suivant**.
3. Sélectionnez soit **Utiliser les références d'ouverture de session actuelles** soit un nom d'utilisateur et un mot de passe ayant des droits d'administrateur de schéma.
4. Cliquez sur **Suivant** pour exécuter Dell Schema Extender.
5. Cliquez sur **Terminer**.

Le schéma est étendu. Pour vérifier l'extension de schéma, utilisez la console de gestion de Microsoft (MMC) et le snap-in du schéma Active Directory pour vérifier ce qui suit :

1 Classes (voir [Tableau 6-1](#) à [Tableau 6-6](#))

1 Attributs ([tableau 6-7](#))

Consultez votre documentation Microsoft pour des informations supplémentaires sur comment activer et utiliser le snap-in du schéma Active Directory de MMC.

Tableau 6-1. Définitions de classes pour les classes ajoutées au schéma d'Active Directory

Nom de classe	Numéro d'identification d'objet (OID) attribué
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tableau 6-2. 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 en tant que dellRacDevice dans Active Directory. Cette configuration permet au DRAC 5 d'envoyer des requêtes de protocole Lightweight Directory Access Protocol (LDAP) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 6-3. 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 6-4. 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	dell sLoginUser dell sCardConfigAdmin dell sUserConfigAdmin dell sLogClearAdmin dell sServerResetUser dell sConsoleRedirectUser dell sVirtualMediaUser dell sTestAlertUser dell sDebugCommandAdmin

Tableau 6-5. 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 6-6. 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 6-7. Liste des attributs ajoutés au schéma d'Active Directory

Nom et description de l'attribut	OID attribué et syntaxe de l'identificateur d'objet	À valeur unique
dellPrivilegeMember Liste des objets dellPrivilege appartenant à cet attribut.	1.2.840.113556.1.8000.1280.1.1.2.1 Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Liste des objets dellRacDevices appartenant à ce rôle. Cet attribut est le lien suivant qui correspond au lien dellAssociationMembers précédent. ID du lien : 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si l'utilisateur a des droits d'ouverture de 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 de 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 de 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 d'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 de 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 de 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 d'accès au 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 de test d'alertes 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 d'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 actuelle du schéma est utilisée pour mettre le schéma à jour.	1.2.840.113556.1.8000.1280.1.1.2.12 Chaîne Ignorer la casse (cis) (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Cet attribut est le type de RAC actuel pour l'objet dellRacDevice et le lien précédent vers le lien suivant dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Chaîne Ignorer la casse (cis) (LDAPTYPE_CASEIGNORESTRING)	TRUE

	1.2.840.113556.1.4.905)	
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien précédent vers l'attribut lié dellProductMembers.	Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
ID du lien : 12071		

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 de gestion de systèmes à l'aide du CD *Dell Systems Management Consoles*, vous pouvez étendre le snap-in en sélectionnant l'option **extension Dell 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 plus d'instructions sur l'installation de Systems Management Software.

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez votre documentation Microsoft.

Installation du pack administrateur

Vous devez installer le pack administrateur sur tous les systèmes qui gèrent les objets 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.

Consultez la section « [Ouverture du snap-in Utilisateurs et ordinateurs Active Directory](#) » pour plus d'informations.

Ouverture du snap-in Utilisateurs et ordinateurs Active Directory

Pour ouvrir le snap-in Utilisateurs et ordinateurs Active Directory, effectuez les étapes suivantes :

1. Si vous êtes connecté au contrôleur de domaine, cliquez sur **Démarrer Outils d'administration** → **Active Directory Utilisateurs et Ordinateurs**.
Si vous n'êtes pas connecté au 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 fonctionnant sous Windows 2000).
3. Cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Sélectionnez le snap-in **Utilisateurs et ordinateurs Active Directory** et cliquez sur **Ajouter**.
5. Cliquez sur **Fermer** et cliquez sur **OK**.

Ajout d'utilisateurs 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 :

- 1 Créez un objet Périphérique RAC
- 1 Créez un objet Privilège
- 1 Créez un objet Association
- 1 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 le nom du nouvel objet. Le nom doit être le même que le nom DRAC 5 que vous tapez à l'[étape a](#) de la section « [Configuration du DRAC 5 avec le schéma étendu d'Active Directory et l'interface Web](#) ».

4. Sélectionnez **Objet Périphérique RAC**.
5. Cliquez sur **OK**.

Création d'un objet Privilège

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

1. Dans la fenêtre **Racine de la console** (MMC), cliquez-droite sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet RAC Dell**.
La fenêtre **Nouvel objet** apparaît.
3. Tapez le nom du 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, consultez le [tableau 4-8](#)).

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 de l'objet Association. Quand vous créez un objet Association, vous devez choisir l'étendue de l'association qui s'applique au type d'objets 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**.
Ceci ouvre la fenêtre **Nouvel objet**.
3. Tapez le nom du 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 fonctionne en mode 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'utilisateur 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'utilisateur lors de l'authentification sur un périphérique RAC. Vous ne pouvez ajouter qu'un seul objet Privilège à un objet Association.

Ajout de privilèges

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

Cliquez sur l'onglet **Produits** pour ajouter un ou plusieurs périphériques RAC à l'association. Les périphériques associés spécifient les périphériques RAC connectés au réseau et 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 le schéma étendu d'Active Directory et l'interface Web

1. Ouvrez une fenêtre de navigateur Web prise en charge.
2. Connectez-vous à l'interface Web du DRAC 5.
3. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
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 **Activer Active Directory**.
 - b. Tapez le **nom de domaine racine**. Le **nom de domaine racine** est le nom pleinement qualifié du domaine racine 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 DRAC**. Ce nom doit être le même que le nom de domaine du nouvel objet RAC que vous avez créé à partir de votre contrôleur de domaine (reportez-vous à l'[étape 3](#) de la section « [Création d'un objet Périphérique RAC](#) »).
 - b. Tapez le **nom de domaine DRAC** (par exemple, drac5.com). N'utilisez pas le nom NetBIOS. Le **nom de domaine DRAC** est le nom de domaine pleinement qualifié du sous-domaine où se trouve l'objet Périphérique RAC.
9. Cliquez sur **Appliquer** pour enregistrer les paramètres Active Directory.
10. Cliquez sur **Retour à la page Menu principal d'Active Directory**.
11. Téléchargez votre certificat d'autorité de certification racine de forêt de domaine dans le DRAC 5.
 - a. Cochez la case **Exporter le certificat d'autorité de certification d'Active Directory**, puis cliquez sur **Suivant**.
 - b. Sur la page **Exportation d'un certificat**, tapez le chemin d'accès au fichier du certificat ou naviguez vers le fichier du certificat.

 **REMARQUE** : La valeur **Chemin d'accès au fichier** affiche le chemin d'accès au fichier relatif au certificat que vous téléchargez. Vous devez taper le chemin de fichier absolu qui inclut le chemin complet et le nom de fichier complet, y compris l'extension du fichier.

Les certificats SSL des contrôleurs de domaine doivent être signés par une autorité de certification racine. Le certificat racine d'une autorité de certification doit être disponible sur la station de gestion qui accède au DRAC 5 (voir « [Exportation d'un certificat d'autorité de certification racine du contrôleur de domaine](#) »).

- c. Cliquez sur **Appliquer**.

Le Web Server du DRAC 5 redémarre automatiquement lorsque vous cliquez sur **Appliquer**.

12. Fermez puis ouvrez une session DRAC 5 pour terminer la configuration de la fonctionnalité Active Directory du DRAC 5.

13. Dans l'arborescence **Système**, cliquez sur **Accès à distance**.

14. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.

La page **Configuration réseau** s'affiche.

15. Si **Utiliser DHCP (pour l'adresse IP du NIC)** est sélectionné dans **Paramètres réseau**, sélectionnez alors **Utiliser DHCP pour obtenir les adresses de serveur DNS**.

Pour entrer manuellement l'adresse IP d'un serveur DNS, désélectionnez **Utiliser DHCP pour obtenir les adresses de serveur DNS** et tapez l'adresse IP de vos serveurs DNS principal et secondaire.

16. Cliquez sur **Appliquer les changements**.

La configuration de la fonctionnalité du schéma étendu d'Active Directory du DRAC 5 est terminée.

Configuration du DRAC 5 avec le schéma étendu d'Active Directory et RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory du DRAC 5 avec le schéma étendu via l'outil CLI RACADM plutôt que via 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 du domaine pleinement qualifié du rac>
racadm config -g cfgActiveDirectory -o cfgADRootDomain <nom du domaine racine pleinement qualifié>
racadm config -g cfgActiveDirectory -o cfgADRacName <nom de domaine du RAC>
racadm sslcertupload -t 0x2 -f <certificat d'autorité de certification racine ADS>
racadm sslcertdownload -t 0x1 -f <certificat SSL du RAC>
```

2. Si DHCP est activé sur le DRAC 5 et que vous voulez utiliser le nom 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 que vous voulez entrer manuellement l'adresse IP DNS, tapez les commandes racadm suivantes :

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP du serveur DNS principal>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP du serveur DNS secondaire>
```

4. Appuyez sur **Entrée** pour terminer la configuration de la fonctionnalité Active Directory du DRAC 5.

Présentation du schéma standard d'Active Directory

Comme illustré dans la [figure 6-4](#), l'utilisation du schéma standard pour l'intégration d'Active Directory exige une configuration sur Active Directory et le DRAC 5. Sur Active Directory, un objet de groupe standard est utilisé comme un groupe de rôles. Un utilisateur ayant accès au DRAC 5 sera membre du groupe de rôles. Pour donner à cet utilisateur accès à une carte DRAC 5 particulière, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cette carte DRAC 5. Contrairement à la solution du schéma étendu, le niveau des rôles et des privilèges est défini sur chaque carte DRAC 5 et non pas dans Active Directory. Jusqu'à cinq groupes de rôles peuvent être configurés et définis dans chaque DRAC 5. Le [tableau 4-15](#) indique les niveaux de privilège des groupes de rôles et le [tableau 6-8](#) indique les paramètres par défaut des groupes de rôles.

Figure 6-4. Configuration du DRAC 5 avec Microsoft Active Directory et le schéma standard

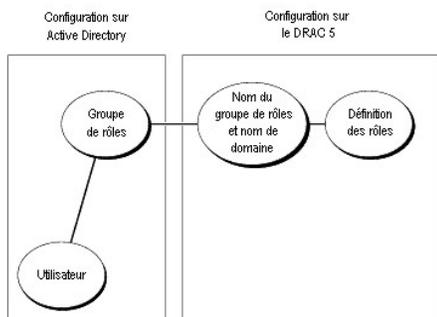


Tableau 6-8. Privilèges par défaut des groupes de rôles

Groupe de rôles	Niveau de privilège par défaut	Droits accordés	Masque binaire
Groupe de rôles 1	Administrateur	Ouvrir une session DRAC, Configurer le DRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des 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 DRAC, Effacer les journaux, Exécuter des 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 DRAC	0x00000001
Groupe de rôles 4	Aucun	Aucun droit attribué	0x00000000
Groupe de rôles 5	Aucun	Aucun droit attribué	0x00000000

REMARQUE : Les valeurs de masque binaire ne sont utilisées que pendant le paramétrage du schéma standard avec RACADM.

Il y a deux manières d'activer le schéma standard d'Active Directory :

1. Avec l'interface utilisateur Web du DRAC 5. Voir « [Configuration du DRAC 5 avec le schéma standard d'Active Directory et l'interface Web](#) ».
1. Avec l'outil CLI RACADM. Voir « [Configuration du DRAC 5 avec le schéma standard d'Active Directory et RACADM](#) ».

Configuration du schéma standard d'Active Directory pour accéder au DRAC 5

Vous devez suivre les étapes suivantes pour configurer Active Directory avant qu'un utilisateur Active Directory puisse avoir accès 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 doivent être configurés sur le DRAC 5 avec l'interface Web ou RACADM (voir « [Configuration du DRAC 5 avec le schéma standard d'Active Directory et l'interface Web](#) » ou « [Configuration du DRAC 5 avec le schéma standard d'Active Directory et RACADM](#) »).
3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour avoir accès au DRAC 5.

Configuration du DRAC 5 avec le schéma standard d'Active Directory et l'interface Web

1. Ouvrez une fenêtre de navigateur Web prise en charge.
2. Connectez-vous à l'interface Web du DRAC 5.
3. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
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 **Activer Active Directory**.
 - b. Tapez le **nom de domaine racine**. Le **nom de domaine racine** est le nom pleinement qualifié du domaine racine 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 le groupe de rôles** apparaît avec le **nom du groupe**, le **domaine du groupe** et les **privileges du groupe de rôles** du groupe de rôles.
10. Tapez le **nom du groupe**. Le nom du groupe identifie le groupe de rôles dans la version d'Active Directory associée à la carte DRAC 5.
11. Tapez le **domaine du groupe**. Le **domaine du groupe** est le nom pleinement qualifié du domaine racine de la forêt.
12. Dans la page **Privileges du groupe de rôles**, définissez les privilèges du groupe.
Le [tableau 4-15](#) décrit les **privileges des groupes de rôles**.
Le [tableau 4-16](#) décrit les **droits des groupes de rôles**. Si vous modifiez des droits, le **privilege du groupe de rôles** actuel (administrateur, utilisateur privilégié ou invité) devient celui d'un groupe personnalisé ou un privilege de rôle de groupes correspondant aux droits modifiés.
13. Cliquez sur **Appliquer** pour enregistrer les paramètres du groupe de rôles.
14. Cliquez sur **Retour à Configuration et gestion d'Active Directory**.
15. Cliquez sur **Retour à la page Menu principal d'Active Directory**.
16. Téléchargez votre certificat d'autorité de certification racine de forêt de domaine dans le DRAC 5.
 - a. Cochez la case **Exporter le certificat d'autorité de certification d'Active Directory**, puis cliquez sur **Suivant**.
 - b. Sur la page **Exportation d'un certificat**, tapez le chemin d'accès au fichier du certificat ou naviguez vers le fichier du certificat.

 **REMARQUE** : La valeur **Chemin d'accès au fichier** affiche le chemin d'accès au fichier relatif au certificat que vous téléchargez. Vous devez taper le chemin de fichier absolu qui inclut le chemin complet et le nom de fichier complet, y compris l'extension du fichier.

Les certificats SSL des contrôleurs de domaine doivent être signés par une autorité de certification racine. Le certificat racine d'une autorité de certification doit être disponible sur votre station de gestion ayant accès au DRAC 5 (voir la section « [Exportation d'un certificat d'autorité de certification racine du contrôleur de domaine](#) »).

 - c. Cliquez sur **Appliquer**.
Le Web Server du DRAC 5 redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
17. Fermez puis ouvrez une session DRAC 5 pour terminer la configuration de la fonctionnalité Active Directory du DRAC 5.
18. Dans l'arborescence **Système**, cliquez sur **Accès à distance**.
19. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.
La page **Configuration réseau** s'affiche.
20. Si **Utiliser DHCP (pour l'adresse IP du NIC)** est sélectionné dans **Paramètres réseau**, sélectionnez **Utiliser DHCP pour obtenir les adresses de serveur DNS**.
Pour entrer manuellement l'adresse IP d'un serveur DNS, désélectionnez **Utiliser DHCP pour obtenir les adresses de serveur DNS** et tapez l'adresse IP de vos serveurs DNS principal et secondaire.
21. Cliquez sur **Appliquer les changements**.
La configuration de la fonctionnalité du schéma standard d'Active Directory du DRAC 5 est terminée.

Configuration du DRAC 5 avec le schéma standard d'Active Directory et RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory du DRAC 5 avec le schéma standard via l'outil CLI RACADM plutôt que via 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 cfgADRootDomain <nom du domaine racine pleinement qualifié>

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

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

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

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

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

```

 **REMARQUE :** Pour des informations sur les valeurs numériques des masques binaires, reportez-vous au [tableau B-4](#).

2. Si DHCP est activé sur le DRAC 5 et que vous voulez utiliser le nom 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 entrer manuellement l'adresse IP DNS, tapez les commandes racadm suivantes :

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

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

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

Activation de SSL sur un contrôleur de domaine

Si vous utilisez l'autorité de certification 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. Installez une autorité de certification racine d'entreprise Microsoft sur un contrôleur de domaine.
 - a. Sélectionnez **Démarrer** → **Panneau de configuration** → **Ajout/Suppression de programmes**.
 - b. Sélectionnez **Ajouter/Supprimer des composants Windows**.
 - c. Dans l'**assistant composants de Windows**, sélectionnez la case **Services de certificats**.
 - d. Sélectionnez **Autorité de certification racine d'entreprise** pour **Type d'autorité de certification** et cliquez sur **Suivant**.
 - e. Entrez **Nom commun de cette autorité de certification**, cliquez sur **Suivant** puis sur **Terminer**.
2. Activez SSL sur chacun de vos contrôleurs de domaine en installant le certificat SSL pour chaque contrôleur.
 - a. Cliquez sur **Démarrer** → **Outils d'administration** → **Politique de sécurité de domaine**.
 - b. Développez le dossier **Stratégie de clé publique**, cliquez-droite sur **Paramètres de demande automatique de certificat** et cliquez sur **Demande de certificat automatique**.
 - c. Dans l'**assistant Création de demandes automatiques de certificats**, cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.
 - d. Cliquez sur **Suivant** puis sur **Terminer**.

Exportation d'un certificat d'autorité de certification racine du contrôleur de domaine

 **REMARQUE :** Si votre système fonctionne sous Windows 2000, les étapes suivantes peuvent varier.

1. Localisez le contrôleur de domaine qui exécute le service d'autorité de certification Microsoft Enterprise.
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 composant snap-in**.
5. Sur la fenêtre **Ajouter/Supprimer un composant logiciel enfichable**, cliquez sur **Ajouter**.

6. Sur la fenêtre **Composant logiciel enfichable 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**, développez le dossier **Personnel** et cliquez sur le dossier **Certificats**.
11. Recherchez le certificat d'autorité de certification racine et cliquez-droite dessus, 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)** pour le 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 en utilisant RACADM, consultez la section « [Configuration du DRAC 5 avec le schéma étendu d'Active Directory et de l'interface Web](#) »

Pour télécharger le certificat à l'aide de l'interface Web, effectuez la procédure suivante :

- a. Ouvrez une fenêtre de navigateur Web prise en charge.
- b. Connectez-vous à l'interface Web du DRAC 5.
- c. Développez l'arborescence **Système** et cliquez sur **Accès à distance**.
- 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 :
 - o Cliquez sur **Parcourir** et sélectionnez le certificat
 - o Dans le champ **Valeur**, tapez le chemin d'accès au certificat.
- g. Cliquez sur **Appliquer**.

Importation du certificat SSL du micrologiciel DRAC 5

Utilisez la procédure suivante pour importer le certificat SSL du micrologiciel DRAC 5 dans toutes les listes de certificats sécurisées de contrôleur de domaine.

 **REMARQUE** : Si votre système fonctionne sous Windows 2000, les étapes suivantes peuvent varier.

 **REMARQUE** : Si le certificat SSL du micrologiciel DRAC 5 est signé par une certification 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 Web Server du DRAC 5. Tous les contrôleurs de DRAC 5 sont expédiés avec un certificat auto-signé par défaut.

Pour accéder au certificat à l'aide de l'interface Web du DRAC 5, sélectionnez **Configuration**→ **Active Directory**→ **Téléchargement du certificat du serveur DRAC 5**.

1. Sur le contrôleur de domaine, ouvrez une fenêtre Console MMC et sélectionnez **Certificats**→ **Autorités de certification racine sécurisées**.
2. Cliquez-droite sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
3. Cliquez sur **Suivant** et recherchez le fichier de certificat SSL.
4. Installez le certificat SSL RAC dans le dossier **Autorité de certification racine sécurisée** de chaque contrôleur de domaine.

Si vous avez installé votre propre certificat, vérifiez que l'autorité qui signe le certificat est présente 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 déterminez si vous voulez que Windows sélectionne automatiquement le lieu de sauvegarde du certificat sur la base du type de certificat, ou naviguez jusqu'au lieu de sauvegarde de votre choix.
 6. Cliquez sur **Terminer** et cliquez sur **OK**.
-

Utilisation d'Active Directory pour ouvrir une session DRAC 5

Vous pouvez utiliser Active Directory pour vous connecter au DRAC 5 à l'aide d'une des méthodes suivantes :

- 1 Interface Web
- 1 RACADM distante
- 1 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 un chaîne de caractères ASCII de 1 à 256 octets.

Le nom d'utilisateur et le nom de domaine ne peuvent pas contenir d'espace ou de caractères spéciaux (comme \, /, or @).

 **REMARQUE :** Vous ne pouvez pas spécifier de noms de domaine NetBIOS, tels que « Amériques », car ces noms ne peuvent pas être résolus.

Questions les plus fréquentes

Le [tableau 6-9](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 6-9. Utilisation du DRAC 5 avec Active Directory : Questions les plus fréquentes

Question	Réponse
Puis-je ouvrir une session DRAC 5 avec Active Directory sur plusieurs arborescences ?	Oui. L'algorithme de requête d'Active Directory du DRAC 5 prend en charge plusieurs arborescences d'une même forêt.
L'ouverture d'une session DRAC 5 avec Active Directory est-elle possible en mode mixte (c-à-d, avec des contrôleurs de domaine de la forêt fonctionnant sous des systèmes d'exploitation différents, comme Microsoft Windows NT® 4.0, Windows 2000 ou Windows Server 2003) ?	Oui. En mode mixte, tous les objets utilisés par la procédure de requête du DRAC 5 (entre autres l'utilisateur, l'objet Périphérique RAC et l'objet Association) doivent être dans le même domaine. Le snap-in Utilisateurs et ordinateurs Active Directory étendu pour Dell vérifie le mode et limite les utilisateurs pour créer des objets à travers les domaines en mode mixte.
L'utilisation du DRAC 5 avec Active Directory prend-elle en charge plusieurs environnements de domaine ?	Oui. Le niveau de la fonction de forêt de domaine doit être en mode natif ou Windows 2003. De plus, les groupes qui font partie de l'objet Association, des objets d'utilisateurs RAC et des objets de périphérique RAC (y compris l'objet Association) doivent être des groupes universels.
Ces objets étendus pour Dell (objets Association Dell, Périphériques RAC Dell et Privilèges Dell) peuvent-ils appartenir à différents domaines ?	L'objet Association et l'objet Privilège doivent être dans le même domaine. Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous force à créer ces deux objets dans le même domaine. D'autres objets peuvent appartenir à différents domaines.
Y a-t-il des limitations pour la configuration SSL des contrôleurs de domaine ?	Oui. Tous les certificats SSL des serveurs Active Directory de la forêt doivent être signés par la même autorité de certification racine puisque le DRAC 5 ne permet de télécharger qu'un seul certificat SSL d'autorité de certification de confiance.
J'ai créé un nouveau certificat de RAC et je l'ai téléchargé ; depuis, l'interface Web ne se lance pas.	Si vous avez utilisé les services de certificats Microsoft pour générer le certificat du RAC, vous avez peut-être choisi Certificat d'utilisateur au lieu de Certificat Web lorsque vous avez créé le certificat. Pour récupérer, générer une CSR puis créer un nouveau certificat Web à partir des services de certificats Microsoft et le charger avec la CLI RACADM du système géré, utilisez les commandes suivantes : <code>racadm sslcsrgen [-g] [-u] [-f {nom de fichier}]</code> <code>racadm sslcertupload -t 1 -f {web_sslcert}</code>
Je n'arrive pas à ouvrir une session DRAC 5 avec l'authentification d'Active Directory ? Qu'est-ce que je peux faire pour résoudre ce problème ?	<ol style="list-style-type: none">1. Vérifiez que vous utilisez le bon nom de domaine utilisateur à l'ouverture de session et que ce n'est pas le nom NetBIOS.2. Si vous avez un compte utilisateur DRAC local, ouvrez une session DRAC 5 à l'aide de vos références locales. Une fois la session ouverte, effectuez les étapes suivantes : <ol style="list-style-type: none">a. Vérifiez que vous avez sélectionné la case Activer Active Directory sur la page de configuration d'Active Directory du DRAC 5.b. Vérifiez que le paramètre DNS est correct sur la page de configuration du réseau du DRAC 5.c. Vérifiez que vous avez téléchargé le certificat Active Directory sur le DRAC 5 à partir de l'autorité de certification racine d'Active Directory.d. Vérifiez les certificats SSL des contrôleurs de domaine pour vous assurer qu'ils n'ont pas expiré.e. Vérifiez que le nom DRAC, le nom de domaine racine et le nom de domaine 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 du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation de la redirection de console de l'interface utilisateur graphique

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Présentation générale](#)
- [Utilisation de la redirection de console](#)
- [Utilisation de Video Viewer](#)
- [Questions les plus fréquentes](#)

Cette section fournit des informations sur l'utilisation de la fonctionnalité de redirection de console du DRAC 5.

Présentation générale

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.

De nos jours, avec les capacités de la mise en réseau et l'Internet, vous n'avez pas besoin d'être assis devant chacun de vos serveurs pour en faire l'entretien de routine. Vous pouvez gérer les serveurs à partir d'une autre ville ou de l'autre bout du monde d'un ordinateur de bureau ou d'un 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 de la station de gestion locale pour contrôler les périphériques correspondants du système géré distant. Cette fonctionnalité peut être utilisée conjointement à la fonctionnalité de média virtuel pour installer les logiciels à distance.

Les règles suivantes s'appliquent à une session de redirection de console :

- 1 Seulement deux sessions de redirection de console simultanées sont prises en charge.
- 1 Une session de redirection de console peut seulement être connectée à un système cible distant.
- 1 Vous ne pouvez pas configurer une session de redirection de console sur le système local.
- 1 Une bande de fréquence de réseau disponible minimale de 1 Mo/s est exigée.

Fréquences d'actualisation de résolutions d'écran prises en charge sur le système géré

Le [tableau 7-1](#) énumère les résolutions d'écran prises en charge et les fréquences d'actualisation correspondantes pour une session de redirection de console qui est exécutée sur le système géré.

Tableau 7-1. Résolutions d'écran prises en charge et fréquences d'actualisation

Résolution d'écran	Fréquence d'actualisation (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. Consultez les sections suivantes pour plus d'informations :
 - « [Navigateurs Web pris en charge](#) »
 - **REMARQUE :** La redirection de console et le média virtuel prennent uniquement en charge les navigateurs 32 bits. L'utilisation de navigateurs 64 bits peut générer des résultats inattendus ou des défaillances.
 - « [Configuration d'un navigateur Web pris en charge](#) »
2. 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**.

Configuration de la redirection de console

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session DRAC 5. Consultez la section « [Accès à l'interface Web](#) » pour plus d'informations.
2. Dans l'arborescence **Système**, cliquez sur **Système**.
3. Cliquez sur l'onglet **Console**, puis sur **Configuration**.
4. Sur la page **Configuration de la redirection de console**, utilisez les informations du [tableau 7-2](#) pour configurer votre session de redirection de console, puis cliquez sur **Appliquer les changements**.

Tableau 7-2. Informations de la page Configuration de la redirection de console

Informations	Description
Activé	Sélectionné = Activé ; Désélectionné = 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 ouvertes.
Numéro de port de clavier et de souris	Valeur par défaut = 5900
Numéro du port vidéo	Valeur par défaut = 5901
Cryptage vidéo activé	Sélectionné = Activé ; Désélectionné = Désactivé
Vidéo du serveur local activée	Sélectionné = Activé ; Désélectionné = Désactivé

Les boutons répertoriés dans le [tableau 7-3](#) sont disponibles sur la page **Configuration de la redirection de console**.

Tableau 7-3. Boutons de la page Configuration de la redirection de console

Propriété	Description
Imprimer	Imprime la page Configuration de la redirection de console .
Actualiser	Recharge la page Configuration de la redirection de console .
Appliquer les changements	Enregistre vos paramètres de configuration.

Ouverture d'une session de redirection de console

Quand vous ouvrez une session de redirection de console, l'application permettant de visualiser le KVM virtuel Dell démarre et le bureau du système distant apparaît dans le visualiseur. Grâce à l'application permettant de visualiser le KVM virtuel, vous pouvez contrôler les fonctions de souris et de clavier du système à partir d'une station de gestion locale ou distante.

Pour ouvrir une session de redirection de console, effectuez les étapes suivantes.

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session DRAC 5. Consultez la section « [Accès à l'interface Web](#) » pour plus d'informations.
2. Dans l'arborescence **Système**, cliquez sur **Système**, puis, sous 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 [l'étape 1](#).

3. Sur la page **Redirection de console**, utilisez les informations de la [tableau 7-4](#) pour garantir qu'une session de redirection de console est disponible.

Tableau 7-4. Informations de la page Redirection de console

Propriété	Description
Redirection de console activée	Oui/Non
Cryptage vidéo activé	Oui/Non
Vidéo du serveur local activée	Oui/Non
Condition	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 ouvertes.
------------------	---

Les boutons répertoriés dans le [tableau 7-5](#) sont disponibles sur la page **Redirection de console**.

Tableau 7-5. 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 cible.
Imprimer	Imprime la page Configuration de la redirection de console .

- Si une session de redirection de console est disponible, cliquez sur **Connecter**.

 **REMARQUE** : Plusieurs boîtes de dialogue peuvent apparaître après le lancement de l'application. Afin d'empêcher l'accès non autorisé à l'application, vous devez naviguer à travers ces boîtes de dialogue pendant trois minutes. Sinon, vous serez invité à relancer l'application.

 **REMARQUE** : Si une ou plusieurs fenêtres d'**alertes de sécurité** apparaissent au cours des étapes suivantes, lisez les informations qu'elles contiennent et cliquez sur **Oui** pour continuer.

La station de gestion se connecte au DRAC 5 et le bureau du système distant apparaît dans l'application de visualiseur KVM numérique de Dell.

- Si deux pointeurs de souris apparaissent sur le bureau du système distant, synchronisez les pointeurs sur la station de gestion et le système distant. Voir « [Synchronisation des pointeurs de souris](#) ».

Désactivation ou activation de la vidéo locale

Pour désactiver ou activer la vidéo locale, effectuez les procédures suivantes :

- Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session DRAC 5. Consultez la section « [Accès à l'interface Web](#) » pour plus d'informations.
- Dans l'arborescence **Système**, cliquez sur **Système**.
- Cliquez sur l'onglet **Console**, puis sur **Configuration**.
- Si vous voulez activer la vidéo locale sur le serveur, sur la page **Configuration de la redirection de console**, cochez la case **Vidéo du serveur local activée** puis cliquez sur **Appliquer les changements**. La valeur par défaut est ACTIVÉE.
- Si vous voulez désactiver la vidéo locale sur le serveur, sur la page **Configuration de la redirection de console**, décochez la case **Vidéo du serveur local activée** et cliquez sur **Appliquer les changements**.

La page **Redirection de console** affiche la condition de la vidéo du serveur local.

 **REMARQUE** : La fonctionnalité Vidéo du serveur local activée est prise en charge sur tous les systèmes PowerEdge x9xx sauf les systèmes PowerEdge SC1435 et 6950.

 **REMARQUE** : Si vous désactivez la vidéo locale sur le serveur, seul le moniteur connecté au serveur local est désactivé.

Utilisation de Video Viewer

L'application Video Viewer 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 clavier et souris à partir de votre station de gestion. Lorsque vous vous connectez au système distant, Video Viewer démarre dans une fenêtre séparée.

Video Viewer 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 Video Viewer apparaît, vous pouvez être amené à régler les commandes suivantes pour visualiser et contrôler correctement le système distant. Ces réglages incluent :

- 1 Accès à la barre de menus du visualiseur
- 1 Réglage de la qualité vidéo
- 1 Synchronisation des pointeurs 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 de bureau du visualiseur.

La barre de menus peut également être activée en appuyant sur la touche de fonction par défaut <F9>. Pour réaffecter cette touche de fonction à une nouvelle fonction, procédez comme suit :

1. Appuyez sur <F9> ou déplacez votre curseur de souris en haut de Video Viewer.
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 d'activation de menu**, cliquez sur le menu déroulant et sélectionnez une autre touche de fonction.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Le [tableau 7-6](#) illustre les principales fonctionnalités qui sont disponibles dans la barre de menus du visualiseur.

Tableau 7-6. 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	Ferme la page Redirection de console .
Afficher	Actualiser	Met à jour toute la fenêtre du système distant.
	Plein écran	Développe l'écran de session d'une fenêtre en 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, effectuez les étapes suivantes : <ol style="list-style-type: none"> 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 de Session Viewer.
	Réglage vidéo manuel	Fournit des commandes individuelles pour régler manuellement la sortie vidéo de Session Viewer. REMARQUE : Le réglage excentré de la position horizontale désynchronise les pointeurs de la souris.
	Options de session	Fournit des réglages de commandes Session Viewer supplémentaires. L'onglet Souris vous permet de sélectionner le système d'exploitation utilisé pour optimiser les performances de la souris pendant la redirection de console. Sélectionnez Windows , Linux ou Aucun . L'onglet Généralités fournit les options suivantes : <ul style="list-style-type: none"> ▮ Mode de transmission au clavier : sélectionnez Transmettre toutes les séquences de touches à la cible pour transmettre les frappes de votre station de gestion au système distant. ▮ Séquence d'activation de menus : sélectionne la touche de fonction qui active la barre de menus du visualiseur. L'onglet Barre d'outils vous permet de régler le Délai de masquage de la barre d'outils entre 1 et 10 secondes.
Aide	-	Active le menu Aide .

Réglage de la qualité vidéo

L'application Video Viewer 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, effectuez les étapes suivantes :

1. Accédez à la barre de menus du visualiseur. Consultez la section « [Accès à la barre de menus du visualiseur](#) ».
2. Cliquez sur **Outils** et sélectionnez **Réglage vidéo automatique**.

La qualité vidéo est recalibrée et le visualiseur de session réapparaît.

Pour régler manuellement la qualité vidéo, effectuez les étapes suivantes :

1. Accédez à la barre de menus du visualiseur. Consultez la section « [Accès à la barre de menus du visualiseur](#) ».
2. Cliquez sur **Outils** et sélectionnez **Réglage vidéo manuel**.
3. Dans la fenêtre **Réglage vidéo**, cliquez sur chaque bouton de réglage vidéo et réglez les commandes, si nécessaire.

Lorsque vous réglez manuellement la qualité vidéo, suivez les instructions suivantes :

- 1 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.
- 1 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 de Video Viewer. 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 pointeurs de souris

Lorsque vous vous connectez à un système PowerEdge 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 pointeur de souris de votre station de gestion, provoquant l'apparition de deux pointeurs de souris dans la fenêtre de Video Viewer.

Pour synchroniser les pointeurs de souris, effectuez les étapes suivantes :

1. Accédez à la barre de menus du visualiseur. Consultez la section « [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 :** Sur les systèmes Linux (Red Hat ou Novell), il existe des problèmes connus de synchronisation de la flèche de la souris. Pour réduire les problèmes de synchronisation de la souris, assurez-vous que tous les utilisateurs utilisent les paramètres de souris par défaut.

Questions les plus fréquentes

Le [tableau 7-7](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 7-7. Utilisation de la redirection de console : Questions les plus fréquentes

Question	Réponse
Est-ce qu'une nouvelle session de vidéo à distance peut être démarrée quand la vidéo locale sur le serveur est désactivée ?	Oui.
Pourquoi la vidéo locale sur le serveur prend-elle 15 secondes pour se désactiver après une requête pour la désactiver ?	Ceci permet à l'utilisateur local d'agir avant que la vidéo ne soit désactivée.
Est-ce qu'il y a un délai quand la vidéo locale est activée ?	Non, une fois que la requête pour activer la vidéo locale est reçue par le DRAC 5, la vidéo est activée immédiatement.
Est-ce que l'utilisateur local peut aussi désactiver la vidéo ?	Oui, un utilisateur local peut utiliser la CLI racadm (locale) pour désactiver la vidéo.
Est-ce que l'utilisateur local peut aussi activer la vidéo ?	Oui, si l'utilisateur a la CLI racadm installée sur le serveur et seulement si l'utilisateur peut avoir accès au serveur avec une connexion RDP, comme les services Terminal Server, telnet ou SSH. L'utilisateur peut alors se connecter au serveur et exécuter racadm (local) 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 RDP, telnet ou SSH. Comment est-ce que je récupère la vidéo locale ?	Dans ce cas, la seule façon de récupérer la vidéo locale est de débrancher le cordon d'alimentation en CA du serveur pour décharger l'alimentation continue du serveur puis de rebrancher le cordon d'alimentation en CA ; la vidéo locale réapparaîtra sur le moniteur du serveur. La configuration du DRAC 5 est également modifiée à la vidéo locale ACTIVÉE (par défaut). Le DRAC 5 doit être reconfiguré si la vidéo locale doit être de nouveau désactivée.
La désactivation de la vidéo locale désactive-t-elle aussi le clavier et la souris locaux ?	Non, la désactivation de la vidéo locale désactive seulement la vidéo du connecteur de sortie du moniteur du serveur ; le clavier et la souris qui sont connectés localement au serveur <i>ne sont pas</i> désactivés.
La désactivation de la vidéo du serveur local désactive-t-elle la vidéo sur la session vKVM	Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de la console distante.

distante ?	
Quels sont les privilèges nécessaires à un utilisateur DRAC 5 pour activer ou désactiver la vidéo du serveur local ?	Tout utilisateur avec des privilèges de configuration DRAC 5 peut activer ou désactiver la vidéo du serveur local.
Comment est-ce que je peux recevoir la condition actuelle de la vidéo du serveur local ?	La condition est affichée sur la page Configuration de la redirection de console de l'interface Web du DRAC 5. La commande CLI <code>racadm racadm getconfig -g cfgRacTuning</code> affiche la condition dans l'objet <code>cfgRacTuneLocalServerVideo</code> . Cette condition se présente à l'utilisateur local sur l'écran LCD du serveur comme « Vidéo ACTIVÉE » ou comme « Vidéo DÉACTIVÉE dans 15 ».
Pourquoi est-ce que parfois je ne vois pas la condition « Vidéo ACTIVÉE » ou « Vidéo DÉACTIVÉE dans 15 » sur l'écran LCD du serveur ?	La condition de la vidéo locale est un message de basse priorité et est masquée quand un événement de serveur de haute priorité se produit. Les messages LCD sont basés sur la priorité ; vous devez résoudre les messages LCD de haute priorité et une fois que l'événement est effacé ou résolu, le prochain message de basse priorité s'affiche. Le message de la vidéo du serveur sur l'écran LCD est à titre d'information.
Où est-ce que je peux recevoir plus d'informations sur les fonctionnalités de la vidéo du serveur local ?	Un document de présentation technique discutant de ces fonctionnalités est disponible sur le site Web de support de Dell à l'adresse support.dell.com .
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 : Il peut être nécessaire de 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, vous devez réinitialiser le DRAC 5 en exécutant la commande <code>racadm racreset</code> .
Je n'arrive pas à voir le bas de l'écran système à partir de la fenêtre de 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 persiste, vous devez réinitialiser le DRAC 5 en exécutant la commande <code>racadm racreset</code> . Si le problème persiste, vous devez réinitialiser le DRAC 5 en exécutant la commande <code>racadm racreset hard</code> .
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 Integrated Devices (Périphériques intégrés) puis USB Controller (Contrôleur USB) . Enregistrez vos changements 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 à jour le pilote vidéo avec le CD <i>Dell PowerEdge Installation and Server Management</i> .
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 avec le CD <i>Dell PowerEdge Installation and Server Management</i> pour avoir les pilotes pris en charge les plus récents 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 à jour le pilote vidéo avec le CD <i>Dell PowerEdge Installation and Server Management</i> .
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 à jour le pilote vidéo avec le CD <i>Dell PowerEdge Installation and Server Management</i> .
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 de redirection de console et ajuster le point de référence. Pour déplacer le point de référence sur la barre de menu du bas de la fenêtre de redirection de console, utilisez la souris et cliquez sur l'un des objets de cette barre.
La souris vKVM n'est pas synchronisée lorsque j'utilise le CD <i>Dell PowerEdge Installation and Server Management</i> 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 n'est pas synchronisée 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 n'est pas synchronisée 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 convertirait en position relative et le comportement ne changerait pas.
Pourquoi la souris n'est-elle pas synchronisée 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 Fermer .

	<ol style="list-style-type: none"> 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 des 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 DRAC 5. Pourquoi ?	<p>Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système dont la fonction de redirection de console est activée dans le BIOS, vous recevez un message de connexion EMS qui vous demande de sélectionner OK pour pouvoir continuer. Vous ne pouvez pas utiliser la souris pour cliquer sur 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.</p> <p>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.</p>
La redirection de console ne montre pas le menu du système d'exploitation dans les versions chinoises, japonaises et coréennes de Microsoft Windows 2000. Pourquoi ?	<p>Sur les systèmes fonctionnant sous Windows 2000 qui peuvent s'amorcer sur plusieurs systèmes d'exploitation, changez le système d'exploitation d'amorçage par défaut en effectuant les étapes suivantes :</p> <ol style="list-style-type: none"> 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 de Démarrage. 5. Dans la case Afficher la liste des systèmes d'exploitation durant, tapez la durée, en secondes, pendant laquelle la liste de choix doit s'afficher avant que le système d'exploitation par défaut démarre automatiquement.
Pourquoi l'indicateur du verrouillage numérique sur ma station de gestion ne reflète-t-il pas la même chose sur le serveur distant ?	Quand on y accède via le DRAC 5, l'indicateur du verrouillage numérique sur la station de gestion ne correspond pas nécessairement à l'état du verrouillage numérique sur le serveur distant. L'état du verrouillage numérique dépend du paramètre sur le serveur distant lorsqu'une session à distance est ouverte et ne tient pas compte de l'état du verrouillage numérique sur la station de gestion.
Pourquoi plusieurs fenêtres de 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 avertissement.
Quelle est la bande de fréquence nécessaire pour exécuter une session de redirection de console ?	Dell recommande une connexion à 5 Mo/s pour une performance optimale. Une connexion à 1 Mo/s suffit pour une performance minimale.
Quelle est la configuration minimale requise de ma station de gestion pour exécuter la redirection de console ?	La station de gestion nécessite un processeur Intel Pentium III 500 MHz avec au moins 256 Mo de mémoire 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.
Pourquoi est-ce que j'ai des problèmes de synchronisation de la souris ?	Sur les systèmes Linux (Red Hat ou Novell), il existe des problèmes connus de synchronisation de la flèche de la souris. Pour réduire les problèmes de synchronisation de la souris, assurez-vous que tous les utilisateurs utilisent les paramètres de souris par défaut.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation et configuration du média virtuel

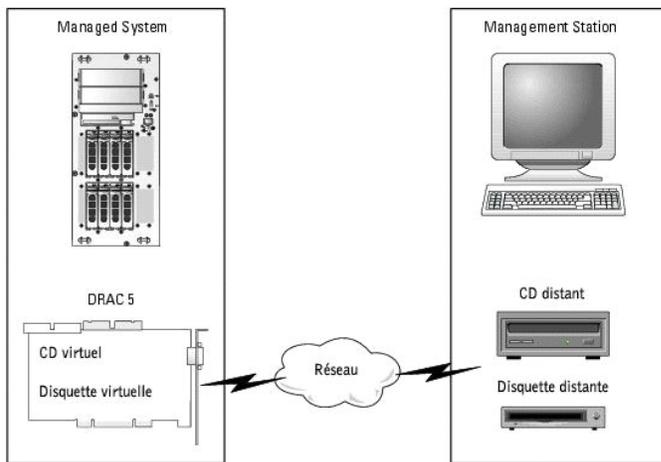
Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Présentation générale](#)
- [Installation du plug-in Média virtuel](#)
- [Exécution du média virtuel](#)
- [Utilisation du disque flash virtuel](#)
- [Utilisation de l'interface de ligne de commande du média virtuel](#)
- [Questions les plus fréquentes](#)

Présentation générale

La fonctionnalité du média virtuel fournit au système géré un lecteur de CD virtuel qui peut utiliser des médias standard à partir de n'importe quel endroit sur le réseau. La [figure 8-1](#) montre l'architecture globale d'un média virtuel.

Figure 8-1. 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 disquettes 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 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 non.

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 Média virtuel est téléchargé à partir du Web Server du DRAC 5 et est automatiquement installé sur la station de gestion. Pour que la fonctionnalité du média virtuel fonctionne correctement, le plug-in Média virtuel doit être installé sur la station de gestion.

Lorsque le média virtuel est connecté, toutes les requêtes d'accès au lecteur de CD ou de disquette virtuel provenant du système géré sont dirigées vers la station de gestion par 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.

Le [tableau 8-1](#) 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 d'amorçage du système.

Tableau 8-1. 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 avec disquette 1.44	CD-ROM, DVD, CDRW, lecteur mixte avec média 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 CD-ROM.

Installation du plug-in Média virtuel

Le plug-in de 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 DRAC 5 et lancé la page de média virtuel, le navigateur télécharge automatiquement le plug-in, si nécessaire. Si le plug-in est installé, la page Média virtuel affiche une liste de disquettes et de disques optiques auxquels le lecteur virtuel peut se connecter.

Station de gestion Windows

Pour exécuter la fonctionnalité de 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 de navigateur sur **Moyen** ou un paramètre inférieur pour activer Internet Explorer et télécharger et installer les contrôles ActiveX signés.

Consultez la section « [Navigateurs Web pris en charge](#) » pour plus d'informations.

En outre, vous devez disposer des privilèges administrateur pour pouvoir installer et utiliser la fonctionnalité Média virtuel. Avant d'installer le contrôle ActiveX, Internet Explorer affichera peut-être 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 de média virtuel sur une station de gestion exécutant le système d'exploitation Linux, installez une version prise en charge de Mozilla ou Firefox. Si le plug-in du média virtuel n'est pas déjà 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 que vous voulez installer le 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 répertoire du navigateur. Si l'ID d'utilisateur n'a pas de droits d'écriture, vous ne pouvez pas installer le plug-in de média virtuel.

Consultez la section « [Navigateurs Web pris en charge](#) » pour plus d'informations.

Exécution du média virtuel

 **AVIS :** N'émettez pas une commande rereset 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 activant une image de disquette, un lecteur de disquette ou un lecteur optique sur votre console de gestion pour 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. Seulement un lecteur pour chaque type de média peut être virtualisé en même temps.

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 via l'interface utilisateur Web

Connexion du média virtuel

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion. Consultez la section « [Navigateurs Web pris en charge](#) ».

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

2. Connectez-vous au DRAC 5 et ouvrez une session. Consultez la section « [Accès à l'interface Web](#) » pour plus d'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 lecteur optique et un 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 de média virtuel.
5. Dans la zone **Attribut**, effectuez les étapes suivantes :
 - a. Dans la colonne **Valeur**, assurez-vous que la valeur de condition **Connecter/Déconnecter** est définie sur **Connecté**.

Si la valeur est sur **Déconnecté**, effectuer les étapes suivantes :

 - o Dans l'onglet **Média**, cliquez sur **Configuration**.
 - o Dans la colonne **Valeur**, assurez-vous que la case **Connecter le média virtuel** est sélectionnée.
 - o Cliquez sur **Appliquer les changements**.
 - o Dans l'onglet **Média virtuel**, cliquez sur **Média virtuel**.
 - o Dans la colonne **Valeur**, assurez-vous que la valeur de condition **Connecter/Déconnecter** est définie sur **Connecté**.
 - o Assurez-vous que la valeur **Condition actuelle** est définie sur **Pas connecté**. Si le champ **Valeur** affiche **Connecté**, vous devez vous déconnecter de l'image ou du lecteur avant de vous reconnecter. Cette condition indique la condition actuelle de la connexion du Média virtuel uniquement sur l'interface Web.
 - o Vérifiez que la valeur **Session active** est **disponible**. Si le champ **Valeur** affiche **Utilisé**, vous devez attendre que la session du média virtuel soit finie ou fermée en allant à l'onglet **Gestion des sessions** sous **Accès à distance** et en fermant la session du média virtuel active. Seule une seule session de média virtuel active est permise à la fois. Cette session peut avoir été créée par une interface Web ou un utilitaire VM-CLI.
 - o Cochez la case **Cryptage activé** pour établir une connexion cryptée entre le système distant et votre station de gestion (si nécessaire).
1. Si vous virtualisez une image de disquette ou une image ISO, sélectionnez **Fichier image de disquette** ou **Fichier image ISO** et entrez 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 les images ou lecteurs virtualisés de la station de gestion. Les images ou lecteurs virtualisés sont tous déconnectés et ne sont plus disponibles sur le système géré.

Connexion et déconnexion du média virtuel

La fonctionnalité de média virtuel du DRAC 5 est fondé 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 peuvent pas voir de 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 interface racadm locale/distante et d'un port série/Telnet. Pour configurer le média virtuel à l'aide d'un navigateur, accédez à la page **Média**, puis **Configuration**, où vous pouvez modifier les paramètres et les appliquer. Vous pouvez aussi spécifier le **Nombre de ports du média virtuel** et le **Nombre de ports SSL du média virtuel**. De plus, vous pouvez activer ou désactiver la fonctionnalité **Disque flash virtuel** et **Un seul démarrage**.

Connexion et déconnexion du média virtuel à l'aide du navigateur Web

Pour connecter le média virtuel, procédez comme suit :

1. Cliquez sur **Système** -> **Média** -> **Configuration**
2. Cochez la case **Valeur** pour **Connexion au média virtuel**
3. Cliquez sur **Appliquer les changements**

Pour déconnecter le média virtuel, procédez comme suit :

1. Cliquez sur **Système** -> **Média** -> **Configuration**
2. Désélectionnez la case **Valeur** pour **Connexion au média virtuel**

3. Cliquez sur **Appliquer les changements**

Connexion et déconnexion du média virtuel à l'aide de RACADM

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

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

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

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

Démarrage à partir du 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 test d'autodiagnostic, accédez à la fenêtre de configuration du BIOS et vérifiez que les lecteurs virtuels sont activés et énumérés dans le bon ordre.

Pour changer le paramètre du BIOS, effectuez les étapes suivantes :

1. Démarrez le système géré.
2. Appuyez sur <F2> pour accéder à la fenêtre de configuration du BIOS.
3. Faites-la dérouler jusqu'à la séquence d'amorçage et appuyez sur <Entrée>.

Dans la fenêtre contextuelle, les lecteurs optiques virtuels et les lecteurs de disquette virtuels sont répertoriés avec les autres périphériques d'amorçage 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 changements et quittez.

Le système géré redémarre.

Le système géré essaie de démarrer à partir d'un périphérique d'amorçage en suivant la séquence d'amorçage. Si le périphérique virtuel est connecté et qu'un média de démarrage est présent, le système démarre sur ce périphérique virtuel. Autrement, le système ignore le périphérique, tout comme un périphérique physique sans média de démarrage.

Installation de systèmes d'exploitation via le média virtuel

Cette section décrit une méthode manuelle et 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. Consultez la section « [Déploiement de votre système d'exploitation via VM-CLI](#) » pour plus d'informations.

1. Vérifiez ce qui suit :
 - 1 Le CD d'installation de votre système d'exploitation est inséré dans le lecteur de CD de la station de gestion.
 - 1 Le lecteur de CD local est sélectionné.
 - 1 Vous êtes connecté aux lecteurs virtuels.
2. Suivez les étapes de la section « [Démarrage à partir du média virtuel](#) » pour configurer le BIOS de sorte qu'il démarre à partir du lecteur de CD qui servira à l'installation.
3. Suivez les instructions à l'écran pour terminer l'installation.

Utilisation du média virtuel lorsque le système d'exploitation du serveur est en cours d'exécution

Systèmes Windows

Sur les systèmes Windows, les lecteurs de média virtuel sont montés automatiquement et configurés avec une lettre de lecteur.

Sous Windows, les lecteurs virtuels s'utilisent de la même façon que les 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 automatés. Si vos lecteurs ne sont pas automatés, 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 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 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 de disque flash virtuel permanent de 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 :

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

 **AVIS :** 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 désactiver 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 partager et de formater USB.

Avant de télécharger une image à partir du navigateur Web de 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 lecteur de 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 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. Allumez le système 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 de média virtuel

L'utilitaire d'interface de ligne de commande de 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 :

- 1 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 support d'image. Lors de la virtualisation de disques physiques, seule une session peut accéder à un disque physique donné à la fois.

- 1 Les périphériques de média amovibles ou les fichiers image qui sont en accord avec les plug-ins de média virtuel
- 1 L'arrêt automatique lorsque l'option de démarrage unique du micrologiciel du DRAC est activée.
- 1 Les communications sécurisées au 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 d'administrateur ou un privilège spécifique de 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 d'utilisateur privilégié pour pouvoir exécuter l'utilitaire VM-CLI.

Pour les systèmes Linux, vous pouvez accéder à l'utilitaire VM-CLI sans privilèges d'administrateur en utilisant la commande **sudo**. Cette commande fournit 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 d'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 CD *Dell OpenManage™ Systems Management Consoles*, qui est inclus avec votre kit Dell OpenManage System Management. Pour installer l'utilitaire, insérez le CD *System Management Consoles* dans votre lecteur de CD et suivez les instructions affichées à l'écran.

Le CD *Systems Management Consoles* 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 CD contient aussi des fichiers lisez-moi, qui fournissent les dernières informations sur les produits logiciels de gestion de systèmes.

De plus, le CD *Systems Management Consoles* 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, consultez la section « [Déploiement de votre système d'exploitation via VM-CLI](#) ».

Options de ligne de commande

L'interface VM-CLI est identique sur les systèmes Linux et Windows. 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 tant pour RACADM que pour les utilitaires VM-CLI.

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

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

Toute la syntaxe de la ligne de commande est sensible à la casse. Consultez la section « [Paramètres VM-CLI](#) » pour plus d'informations.

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

- 1 La connexion VM-CLI est interrompue pour une raison ou une autre.
- 1 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 terminer le processus.

Paramètres VM-CLI

Adresse IP du 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) 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 au média virtuel avec le DRAC 5 cible. Si vous entrez une adresse IP ou un nom DDNS non valide, un message d'erreur apparaît et la commande est terminée.

Si le <port SSL du RAC> est omis, le port 443 (port par défaut) est utilisé. À moins que le port SSL par défaut du DRAC 5 n'ait été modifié, le port SSL optionnel n'est pas obligatoire.

Nom d'utilisateur DRAC 5

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

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

Le <nom d'utilisateur DRAC> doit avoir les attributs suivants :

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

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

Mot de passe utilisateur DRAC

```
-p <mot de passe d'utilisateur 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 se termine.

Périphérique de disquette ou disque ou fichier image

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

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

Ce paramètre spécifie le périphérique ou le fichier qui fournit le média de disquette ou 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 devrait pas être remplacé.

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 se termine.

Périphérique de CD/DVD ou fichier image

```
-c {<nom de périphérique> | <fichier image>}
```

où <nom de périphérique> est une lettre de lecteur de CD/DVD valide (systèmes Windows) ou un nom de fichier de périphérique de CD/DVD valide (systèmes Linux) et <fichier image> est le nom de fichier et le chemin d'un fichier image ISO-9660 valide.

Ce paramètre spécifie le périphérique ou le fichier qui fournira le média de CD/DVD-ROM virtuel :

Par exemple, un fichier image est spécifié comme :

```
-c c:\temp\mydvd.img (systèmes Windows)
```

```
-c /tmp/mydvd.img (systèmes Linux)
```

Par exemple, un périphérique est spécifié comme :

-c d:\ (systèmes 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 découverte, un message d'erreur est répertorié et la commande se termine.

Spécifiez au moins un type de média (lecteur de disquette ou de CD/DVD) avec la commande, à moins que seules des options de commutation ne soient fournies. Le cas échéant, un message d'erreur s'affiche et la commande se termine en générant une erreur.

Affichage de la version

-v

Ce paramètre est utilisé pour afficher la version de l'utilitaire VM-CLI. Si aucune autre option de non-commutateur n'est fournie, la commande se termine 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 se termine 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 :

- 1 stderr/stdout redirection : redirige l'impression de l'utilitaire vers un fichier.

Par exemple, le caractère plus grand que (>), suivi par un nom de fichier, remplace le fichier indiqué par l'impression 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.

- 1 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, comme elle permet de procéder au 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 terminé). Lorsque plusieurs instances VM-CLI sont démarrées de cette manière et une ou plusieurs instances de commande doivent être terminées manuellement, utilisez les équipements spécifiques au système d'exploitation pour énumérer et terminer les processus.

Codes de retour VM-CLI

0 = aucune erreur

1 = connexion impossible

2 = erreur de ligne de commande VM-CLI

3 = la connexion du micrologiciel du RAC a été coupée

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

Questions les plus fréquentes

Le [tableau 8-2](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 8-2. Utilisation d'un média virtuel : Questions les plus fréquentes

--	--

Question	Réponse
Je remarque parfois que ma connexion de client au Média virtuel est interrompue. Pourquoi ?	Si le délai d'attente du réseau expire, le micrologiciel 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 section « Systèmes d'exploitation pris en charge » pour obtenir la liste des systèmes d'exploitation pris en charge.
Quels sont les navigateurs Web pris en charge par le DRAC 5 ?	Vous trouverez une liste des navigateurs Web pris en charge dans la section « Navigateurs Web pris en charge ».
Pourquoi m'arrive-t-il de perdre parfois ma connexion client ?	<ol style="list-style-type: none"> Vous pouvez parfois perdre votre connexion client si le réseau est lent ou si vous changez de CD dans le lecteur de CD du système client. Par exemple, si vous changez de 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 temps imparti et la connexion peut être perdue si le système client prend trop longtemps avant d'être prêt pour lire le CD. Si une connexion est perdue, reconnectez-vous à partir de l'interface utilisateur graphique et continuez l'opération précédente. En cas de dépassement du délai d'attente du réseau, le micrologiciel 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 <code>usbstor.sys</code> à partir du site Web de support de Microsoft, à l'adresse support.microsoft.com , et exécutez uniquement le programme 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 ?	Si le disque flash virtuel est activé et ne contient pas d'image valide ; par exemple, 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 de 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 CD <i>Installation de Dell PowerEdge et Server Management</i> et d'une connexion réseau 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 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 à la 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 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 : <ol style="list-style-type: none"> 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 pouvoir démarrer à partir de ma clé USB ?	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 : <pre>sys a: x: /s</pre> <p>où « x: » est la clé USB que vous voulez utiliser comme clé de démarrage.</p> <p>Vous pouvez également utiliser l'utilitaire d'amorçage Dell pour créer un clé USB d'amorçage. Cet utilitaire n'est compatible qu'avec les clés USB de marque Dell. Pour télécharger l'utilitaire, lancez un navigateur Web pris en charge, naviguez vers le site Web de support de Dell à l'adresse support.dell.com et recherchez « R122672.exe ».</p>
AI-je besoin de droits d'administrateur pour installer le plug-in ActiveX ?	Vous devez disposer de droits administrateur ou de droits d'utilisateur privilégié sur les systèmes Windows pour pouvoir installer le plug-in 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 des navigateurs pour pouvoir installer le plug-in du média virtuel.
Je n'arrive pas à trouver mon lecteur de disquette virtuel sur un système fonctionnant sous Red Hat Enterprise Linux ou sous SUSE Linux. Mon média virtuel est connecté et je suis connecté à ma disquette à distance. Que dois-je faire ?	Certaines versions de Linux n'installent pas automatiquement le lecteur de disquette virtuel et le lecteur de CD virtuel de la même manière. Pour installer le lecteur de disquette virtuel, recherchez le nœud de périphérique que Linux affecte au lecteur de disquette virtuel. Procédez comme suit pour rechercher et installer correctement le lecteur de disquette virtuel : <ol style="list-style-type: none"> Ouvrez une invite de commande Linux et exécutez la commande suivante : <pre>grep "Virtual Floppy" /var/log/messages</pre> Recherchez la dernière entrée de ce message et notez l'heure. À l'invite de Linux, exécutez la commande suivante :

	<pre>grep "hh:mm:ss" /var/log/messages</pre> <p>où :</p> <p>hh:mm:ss est l'heure du message renvoyé par grep à l'étape 1.</p> <ol style="list-style-type: none"> 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 : <pre>mount /dev/sdx /mnt/floppy</pre> <p>où :</p> <p>/dev/sdx est le nom du périphérique trouvé à l'étape 4</p> <p>/mnt/floppy est le point de montage.</p>
<p>Quels types de systèmes de fichiers sont pris en charge sur mon lecteur de disquette virtuel ou sur le disque flash virtuel ?</p>	<p>Votre lecteur de disquette virtuel ou disque flash virtuel prend en charge les systèmes de fichiers FAT16 ou FAT32.</p>
<p>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 ?</p>	<p>Les mises à jour de micrologiciel entraînent une réinitialisation du DRAC 5, une interruption de la connexion à distance et la désinstallation des lecteurs virtuels. Les lecteurs réapparaîtront une fois la réinitialisation du DRAC terminée.</p>
<p>En activant ou en désactivant le disque flash virtuel, j'ai remarqué que tous mes lecteurs virtuels ont disparu puis ont réapparu. Pourquoi ?</p>	<p>La désactivation ou l'activation du disque flash virtuel entraîne une réinitialisation USB et déconnecte puis reconnecte tous les lecteurs virtuels au bus USB.</p>

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation de l'interface de ligne de commande RACADM

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

- [Utilisation d'une console série ou Telnet](#)
- [Utilisation de RACADM](#)
- [Configuration de plusieurs cartes DRAC 5](#)
- [Utilisation de l'utilitaire RACADM pour configurer le DRAC 5](#)
- [Questions les plus fréquentes](#)

La console série/Telnet/SSH fournit un jeu de commandes racadm. Les commandes racadm permettent d'accéder aux fonctionnalités textuelles prises en charge par l'interface Web du DRAC 5.

RACADM vous permet de configurer et de gérer votre DRAC 5 localement ou à distance. RACADM est exécuté sur la station de gestion et le système géré. RACADM est inclus sur le CD *Dell Systems Management Consoles*.

Vous pouvez utiliser RACADM pour écrire des scripts qui configurent automatiquement plusieurs DRAC 5. Pour plus d'informations sur la configuration de plusieurs DRAC 5, consultez la section « [Configuration de plusieurs cartes DRAC 5](#) ».

Cette section fournit les informations suivantes :

- 1 Utilisation des commandes **série** et **racadm**. Consultez la section « [Utilisation d'une console série ou Telnet](#) » ou « [Utilisation de RACADM](#) »
- 1 Configuration de votre DRAC5 à l'aide de la commande **racadm**
- 1 Utilisation du fichier de configuration racadm pour configurer plusieurs cartes DRAC 5

Utilisation d'une console série ou Telnet

Vous pouvez exécuter les commandes série du [tableau 9-1](#) à distance à l'aide de RACADM ou de l'invite de commande de la console série/Telnet/SSH.

Ouverture d'une session DRAC 5

Une fois le logiciel d'émulation du terminal et le BIOS du nœud géré de votre station de gestion configurés, effectuez les étapes suivantes pour ouvrir une session DRAC 5 :

1. Ouvrez une session 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 DRAC 5.

Lancement d'une console texte

Lorsque vous avez ouvert une session 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 en même temps.

Pour vous connecter à la console de 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 sur le port COM2 des serveurs et évite le DRAC 5. Pour reconnecter le DRAC 5 sur le port série, appuyez sur <Échap><Maj><9>. Les débits en bauds du port COM2 du nœud 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 de terminal client sur 25.

La taille par défaut (et maximale) du tampon de l'historique est 8192 caractères. Vous pouvez réduire cette valeur avec la commande :

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

Utilisation de RACADM

Vous pouvez exécuter les commandes RACADM localement ou à distance de l'invite de commande d'une console série ou Telnet, ou d'une invite de commande normale.

Utilisez la commande **racadm** pour configurer les propriétés du DRAC 5, effectuer les tâches de gestion à distance ou récupérer un système en panne.

Pour afficher la liste des sous-commandes **racadm** à l'aide de **RACADM**, tapez :

```
racadm help
```

La liste des sous-commandes inclut toutes les commandes qui sont prises en charge par le DRAC 5.

Sans options, la commande **racadm** affiche des informations d'ordre général. Tapez `racadm help` pour afficher la liste de toutes les sous-commandes disponibles. Tapez `racadm help <sous-commande>` pour énumérer les options de syntaxe et de ligne de commande pour la sous-commande.

Les sections suivantes donnent des informations sur comment utiliser les commandes **racadm**.

Utilisation de RACADM à distance

REMARQUE : Configurez l'adresse IP du DRAC 5 avant d'utiliser la fonction d'accès à distance **racadm**. Pour plus d'informations sur la configuration de votre DRAC 5 et une liste des documents associés, consultez la section « [Installation et configuration du DRAC 5](#) ».

RACADM fournit une option 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 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 : La fonction d'accès à distance **racadm** n'est prise en charge que sur les stations de gestion. Voir « [Navigateurs Web pris en charge](#) » pour plus d'informations.

REMARQUE : Lorsque vous utilisez la capacité à distance de **racadm**, vous devez avoir le droit d'écrire dans les dossiers utilisés par les sous-commandes **racadm** pour des opérations de fichier, par exemple :

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

ou

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

Synopsis de RACADM

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

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

```
racadm -i -r <adresse IP RAC>:<port> <sous-commande> <options de sous-commande>
```

Options de RACADM

Le [tableau 9-1](#) répertorie les options de la commande **racadm**.

Tableau 9-1. Options de la commande **racadm**

Option	Description
-r <racIpAddr>	Spécifie l'adresse IP distante du contrôleur.
-r <racIpAddr>:<numéro de port>	Utilisez :<numéro de port> si le numéro de port du DRAC 5 n'est pas le port par défaut (443)
-i	Ordonne à racadm de demander de manière interactive à l'utilisateur son nom d'utilisateur et son mot de passe.
-u <usrName>	Spécifie le nom d'utilisateur qui sert à authentifier la transaction de commandes. Si l'option -u est utilisée, l'option -p doit être utilisée et l'option -i (interactive) n'est pas autorisée.
-p <password>	Spécifie le mot de passe qui sert à authentifier la transaction de commande. Si l'option -p est utilisée, l'option -i n'est pas autorisée.

Activation et désactivation de la fonction d'accès à distance racadm

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

Par défaut, la fonction d'accès à distance 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 d'accès à distance, tapez :

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

Sous-commandes RACADM

Le [tableau 9-2](#) fournit une description de chaque sous-commande racadm que vous pouvez exécuter dans RACADM. Pour obtenir une liste détaillée de toutes les sous-commandes racadm, y compris la syntaxe et les entrées valides, consultez la section « [Présentation de la sous-commande RACADM](#) ».

Lorsque vous tapez une sous-commande RACADM, utilisez comme préfixe de commande racadm. Par exemple :

```
racadm help
```

Tableau 9-2. 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 de 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 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 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 les informations actuelles 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	Obtient 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.
clrssel	Efface toutes les entrées du journal des événements système.
gettracelog	Affiche le journal de suivi 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 d'autorité de certification ou un certificat du serveur sur le DRAC 5.
sslcertdownload	Télécharge un certificat d'autorité de certification.
sslcertview	Affiche un certificat d'autorité de certification ou un certificat de serveur du DRAC 5.
testemail	Force le DRAC 5 à envoyer un e-mail en passant par le NIC du DRAC 5.
testtrap	Force le DRAC 5 à envoyer un SNMP en passant par le NIC du DRAC 5.
vmdisconnect	Force la déconnexion du média virtuel.
vmkey	Restaure la valeur par défaut de la taille du disque flash virtuel (16 Mo).

Messages d'erreur racadm

Pour des informations sur les messages d'erreur de la CLI racadm, consultez la section « [Questions les plus fréquentes](#) » de ce chapitre.

Configuration de plusieurs cartes DRAC 5

Utilisez 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 l'ID de l'objet, 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 DRAC 5 uniques (comme l'adresse IP statique) qui doivent être modifiées avant d'exporter le fichier vers d'autres cartes DRAC 5.

Pour configurer plusieurs cartes DRAC 5, effectuez les procédures suivantes :

1. Utilisez RACADM pour effectuer une requête sur le DRAC 5 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 monfichier.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 monfichier.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 :

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

La sous-commande `config` charge les informations dans d'autres DRAC 5. Utilisez `config` pour synchroniser la base de données des utilisateurs et des mots de passe avec Server Administrator

Le fichier de configuration initial, `racadm.cfg`, est nommé par l'utilisateur. Dans l'exemple suivant, le fichier de configuration s'appelle `monfichier.cfg`. Pour créer ce fichier, tapez la commande suivante à l'invite de commande :

```
racadm getconfig -f monfichier.cfg
```

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

Création d'un fichier de configuration 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`. Le fichier de configuration est un fichier texte simple qui permet à l'utilisateur de construire un fichier de configuration (semblable à un fichier `.ini`) et de configurer le DRAC 5 avec ce fichier. Vous pouvez utiliser n'importe quel nom de fichier, et le fichier ne nécessite pas d'extension `.cfg` (même si on le désigne par cette extension dans cette sous-section).

Le fichier `.cfg` peut être :

- 1 Créé
- 1 Obtenu à partir d'une commande `racadm getconfig -f <nom de fichier>.cfg`
- 1 Obtenu à partir de la commande `racadm getconfig -f <nom de fichier>.cfg`, puis modifié

 **REMARQUE :** Consultez la section « [getconfig](#) » pour des informations sur la commande `getconfig`.

Le fichier `.cfg` est d'abord analysé pour vérifier que des noms de groupes et d'objets valides sont présents et que les règles de syntaxe de base sont suivies. Les erreurs sont indiquées avec le numéro de ligne dans laquelle l'erreur a été détectée et un message simple explique le problème. Tout le fichier est analysé et toutes les erreurs sont affichées. Il n'y a pas d'écriture sur le DRAC 5 si une erreur est trouvée dans le fichier `.cfg`. L'utilisateur doit corriger toutes les erreurs avant que la configuration puisse se faire. L'option `-c` peut être utilisée avec la sous-commande `config`, qui ne vérifie que la syntaxe et n'effectue pas d'écriture sur DRAC 5.

Suivez ces instructions lorsque vous créez un fichier `.cfg` :

- 1 Si l'analyseur rencontre un groupe indexé, c'est la valeur de l'objet ancré qui différencie les différents index.

L'analyseur lit tous les index du DRAC 5 pour ce groupe-là. 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.

- 1 L'utilisateur ne peut pas spécifier d'index désiré dans un fichier `.cfg`.

Comme les index peuvent être créés et supprimés, le groupe peut devenir fragmenté petit à petit avec des index utilisés et inutilisés. Si un index est présent, il est modifié. Si aucun index n'est présent, le premier index disponible est utilisé. Cette méthode permet une certaine flexibilité lors de l'ajout d'entrées indexées où l'utilisateur n'a 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.

- 1 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 appropriés.

- 1 **AVIS :** Utilisez la sous-commande `racresetcfg` pour rétablir les paramètres par défaut de la base de données et du NIC du DRAC 5 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

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

Une ligne de commentaire *doit* commencer dans la colonne 1. Un caractère « # » dans toute autre colonne est traité comme un caractère #.

Certains paramètres de modem peuvent inclure les caractères # dans leur chaîne de caractères. Dans ce cas, un caractère d'échappement n'est pas nécessaire. Vous pouvez générer un fichier `.cfg` à partir d'une commande `racadm getconfig -f <nom de fichier>.cfg`, puis exécuter une commande `racadm config -f <nom de fichier>.cfg` sur un autre DRAC 5, sans ajouter de caractères d'échappement.

Exemple :

```
#
# c'est un commentaire

[cfgUserAdmin]

cfgUserAdminPageModemInitString=<Initialisation du modem # pas un commentaire>
```

- 1 Toutes les entrées de groupes doivent être encadrées de caractères « [» et «] ».

Le caractère « [» du début dénotant un nom de groupe *doit* commencer dans la colonne 1. Le nom de groupe *doit* être spécifié avant les objets de 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 la section « [Définitions des groupes et des objets de la base de données de propriétés d'un 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}
```

- 1 Tous les paramètres sont spécifiés en tant que paires « objet = valeur » sans espace entre l'objet, le signe = et la valeur.

Les espaces blancs qui sont inclus après la valeur sont ignorés. Un espace blanc à l'intérieur d'une chaîne de caractères de valeur n'est pas modifié. Tout caractère à droite du « = » est pris tel quel (par exemple, un deuxième « = », ou un « # », « [», «] », et ainsi de suite). Ces caractères sont des caractères de script de conversation de modem valides.

Consultez l'exemple du puce précédente.

- 1 L'analyseur `.cfg` ignore une entrée d'objet d'index.

L'utilisateur *ne peut pas* spécifier l'index à utiliser. Si l'index existe déjà, s'il est utilisé ou autre, 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.

- 1 **REMARQUE :** L'utilisateur peut créer manuellement un groupe indexé à l'aide de la commande suivante :
`racadm config -g <nom de groupe> -o <objet ancré> -i <index 1-16> <nom d'ancre unique>`

- 1 La ligne d'un groupe indexé *ne peut pas* être supprimée d'un fichier `.cfg`.

L'utilisateur doit supprimer un objet indexé manuellement avec la commande suivante :

```
racadm config -g <nom du groupe> -o <nom de l'objet> -i <index de 1 à 16> ""
```

 **REMARQUE :** Une chaîne de caractères nulle (identifiée par deux caractères "") ordonne au DRAC 5 de supprimer l'index du groupe indiqué.

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

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

- 1 Pour les groupes indexés, l'ancre d'objet *doit* être le premier objet après les crochets « [] ». Voici des exemples de groupes actuellement indexés :

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<NOM_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 pour votre fichier `.cfg`.

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 « [] » reste avec les deux entrées `<variable>=valeur` correspondant au changement d'adresse IP.

Par exemple :

```
#
# Groupe d'objets "cfgLanNetworking"
#
```

```
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Le fichier sera mis à jour de la manière suivante :

```
#
# Groupe d'objets "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# commentaire, le reste de cette ligne est ignorée
cfgNicGateway=10.35.9.1
```

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

Utilisez ce fichier pour télécharger des changements généraux ou pour configurer de nouveaux systèmes par le réseau.

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

Utilisation de l'utilitaire RACADM pour configurer le DRAC 5

 **REMARQUE :** Vous devez être connecté 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 :

- 1 Créez un fichier de commandes `racadm`, puis exécutez ce fichier sur chaque système géré, en vous servant des exemples de RACADM de cette section pour vous guider.
- 1 Créez le fichier de configuration du DRAC 5 comme le décrit la section « [Présentation de la sous-commande RACADM](#) » puis exécutez la sous-commande `racadm config` sur chaque système géré en utilisant 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.

 **AVIS :** Soyez prudent lorsque vous utilisez la commande `racresetcfg`, car les valeurs d'origine de *tous* les paramètres de configuration sont restaurées. Toute modification précédente est alors perdue.

 **REMARQUE :** Les utilisateurs peuvent être activés et désactivés à tout moment. Par conséquent, un utilisateur peut avoir un nombre d'index différent sur chaque 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 tous les 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 intéressants 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. S'il y a un nom après le « = », 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 « # ». Si vous utilisez la commande `racadm config -f racadm.cfg` pour spécifier un nombre de groupes/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 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 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 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 nulle de guillemets ("") donne l'ordre au DRAC 5 de supprimer la configuration utilisateur à l'index indiqué et de restaurer les valeurs d'usine par défaut de la configuration utilisateur.

Test d'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'alertes par e-mail pour garantir que le RAC peut correctement envoyer des alertes par e-mail sur le réseau.

```
racadm testemail -i 2
```

 **REMARQUE :** Assurez-vous que les paramètres SMTP et Alerte par e-mail sont configurés avant de tester la fonctionnalité d'alertes par e-mail. Consultez la section « [Configuration des alertes par e-mail](#) » pour plus d'informations.

Test de la fonctionnalité d'alertes par interruption SNMP RAC

La fonctionnalité d'alertes par interruption SNMP 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'alertes par interruption SNMP RAC.

```
racadm testtrap -i 2
```

Avant de tester la fonctionnalité d'alertes par interruption SNMP RAC, assurez-vous que les paramètres d'interruption et SNMP sont configurés correctement. Consultez 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 ayant des droits d'administration spécifiques (autorisation basée sur le rôle), commencez par rechercher un index utilisateur disponible en effectuant les étapes de la section « [Avant de commencer](#) ». Ensuite, tapez les lignes de commande suivantes avec le nouveau nom d'utilisateur et le nouveau mot de passe.

 **REMARQUE :** Consultez le [tableau B-2](#) pour une liste des valeurs de masque binaire valides pour 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 de privilège d'utilisateur>
```

Configuration des propriétés du 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` afin de l'activer.

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

Les commandes fournissent la même fonctionnalité de configuration que l'option ROM à l'amorçage lorsque vous êtes invité à taper <Ctrl><e>. Pour des informations supplémentaires sur la configuration des propriétés réseau avec l'option ROM, consultez la section « [Configuration des propriétés du réseau du DRAC 5](#) ».

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

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
```

```
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

 **REMARQUE :** Si la commande `cfgNicEnable` est définie sur 0, le LAN du DRAC 5 est désactivé même si DHCP est activé.

Modes DRAC

Le DRAC 5 peut être configuré dans un des trois modes suivants :

- 1 Dédié
- 1 Partagé
- 1 Partagé avec basculement

Le [tableau 9-3](#) fournit une description de chaque mode.

Tableau 9-3. 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

Le [tableau 9-4](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 9-4. Utilisation des commandes série et racadm : Questions les plus fréquentes

Question	Réponse
<p>Une fois le DRAC 5 réinitialisé (avec la commande <code>racadm racreset</code>), j'envoie une commande et le message suivant s'affiche :</p> <pre>racadm <nom de commande> Transport: ERROR: (RC=-1)</pre> <p>Qu'est-ce que ce message signifie ?</p>	<p>Vous devez attendre que le DRAC 5 soit complètement réinitialisé avant d'envoyer une autre commande.</p>
<p>Lorsque j'utilise les commandes et les sous-commandes <code>racadm</code>, il y a des erreurs que je ne comprends pas.</p>	<p>Une ou plusieurs des erreurs suivantes peuvent survenir lorsque vous utilisez les commandes et les sous-commandes <code>racadm</code> :</p> <ul style="list-style-type: none"> 1 Messages d'erreur locaux : problèmes de syntaxe, d'erreurs typographiques et de noms incorrects. <p>Exemple :</p> <pre>ERROR: <message></pre>
<p>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.</p>	<p>Effacez le tableau ARP sur votre système.</p>

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Glossaire

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20

Active Directory

Active Directory est un système central et standard qui automatise la gestion réseau des données utilisateur, la sécurité, les ressources distribuées et permet d'interopérer avec d'autres répertoires. Active Directory est conçu pour fonctionner dans des environnements de réseau distribués.

adresse MAC

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

AGP

Abréviation de Accelerated Graphics Port (port graphique accéléré), une spécification du bus qui permet aux cartes vidéo d'accéder plus rapidement à la mémoire du système principal

ARP

Sigle de 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 de 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.

autorité de certification

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

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.

CD

Abréviation de Compact Disc (disque compact).

CHAP

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

CIM

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

CLI

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

CLP

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

CSR

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

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 d'adressage par domaine).

DRAC 5

Abréviation 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 universel), 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 de Intelligent Chassis Management Bus (bus de gestion intelligente du châssis).

ICMP

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

IPMB

Abréviation de Intelligent Platform Management Bus (bus de gestion de plateforme intelligente), un bus utilisé dans la technologie de gestion de systèmes.

IPMI

Abréviation de Intelligent Platform Management Interface (interface de gestion de plateforme 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, un taux de transfert des données.

LAN

Abréviation de Local Area Network (réseau local).

LDAP

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

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 nœud 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, un taux de transfert des données.

MIB

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

MI

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

NAS

Abréviation de Network Attached Storage (stockage connecté au 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.

OID

Abréviation de Object Identifier (identificateur d'objet).

PCI

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

POST

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

PPP

Abréviation de protocole point à point, un protocole Internet standard pour transmettre des 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.

RPM

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

SAC

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

SAP

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

schéma étendu

Solution utilisée avec Active Directory pour configurer l'accès utilisateur au DRAC 5 ; elle utilise des objets Active Directory définis par Dell.

schéma standard

Solution utilisée avec Active Directory pour configurer l'accès utilisateur au DRAC 5 ; elle utilise uniquement des objets de groupe Active Directory.

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 une connexion 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 nœuds sur un réseau IP. Les DRAC 5 sont des périphériques gérés par SNMP (nœuds).

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 réseau et de couche de transport.

TFTP

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

UPS

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

USB

Abréviation de Universal Serial Bus (bus série universel).

UTC

Abréviation de 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 global).

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Guide d'utilisation du micrologiciel Dell™ Remote Access Controller 5, version 1.20



REMARQUE : Une REMARQUE indique des informations importantes qui vous permettent de mieux utiliser votre ordinateur.



AVIS : Un AVIS vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

**Les informations de ce document sont sujettes à modification sans préavis.
© 2007 Dell Inc. Tous droits réservés.**

Toute reproduction, de quelque manière que ce soit, sans l'autorisation écrite de Dell Inc. est strictement interdite.

Marques utilisées dans ce texte : *Dell*, le logo *DELL*, *Dell OpenManage* et *PowerEdge* sont des marques de Dell Inc. ; *Microsoft*, *Active Directory*, *Internet Explorer*, *Windows*, *Windows NT* et *Windows Server* sont des marques déposées et *Windows Vista* est une marque de Microsoft Corporation ; *Red Hat* est une marque déposée de Red Hat, Inc. ; *Novell* et *SUSE* sont des marques déposées de Novell Corporation. *Intel* est une marque déposée de Intel Corporation ; *UNIX* est une marque déposée de The Open Group aux États-Unis d'Amérique et dans d'autres pays.

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

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

[Retour à la page du sommaire](#)