Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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.

Mars 2008 Rev. A01

Retour à la page du sommaire

Présentation de la sous-commande RACADM

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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

---

help

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

Interfaces prises en charge

- RACADM locale

---

config

Le tableau A-2 décrit les sous-commandes **config** et **getconfig**.

Tableau A-2. config / getconfig

Sous-commande	Définition
config	Configure iDRAC.
getconfig	Récupère les données de configuration iDRAC.

Synopsis

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

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

Interfaces prises en charge

- RACADM locale

Description

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

Entrées

Le tableau A-3 décrit les options de la sous-commande **config**.

Tableau A-3. Options et descriptions de la sous-commande config.

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

Résultat

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

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

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

Exemples

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.110`

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

- `racadm config -f myrac.cfg`

  Configure ou reconfigure iDRAC. Le fichier **myrac.cfg** peut être créé à l'aide 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 de mots de passe. Pour inclure des mots de passe dans le fichier, vous devez les entrer manuellement. Si vous souhaitez supprimer les mots de passe du fichier **myrac.cfg** lors de la configuration, utilisez l'option **-p**.

---

getconfig

La sous-commande **getconfig** vous permet de récupérer les paramètres de configuration iDRAC un par un ou de récupérer et d'enregistrer dans un fichier l'ensemble des groupes de configuration iDRAC.

Entrées

Le tableau A-4 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-4. Options de la sous-commande getconfig

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

Résultat

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

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

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

Exemples

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f myrac.cfg`

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

- `racadm getconfig -h`

  Affiche la liste des groupes de configuration disponibles sur iDRAC.

- `racadm getconfig -u root`

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

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

  Affiche l'instance de groupe d'utilisateurs dans l'index 2 avec des informations détaillées 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

- RACADM locale

---

getssninfo

Le tableau A-5 décrit la sous-commande **getssninfo**.

Tableau A-5. Sous-commande getssninfo

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

Synopsis

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

Description

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

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

Interfaces prises en charge

- RACADM locale

Entrées

Le tableau A-6 décrit les options de la sous-commande **getssninfo**.

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

Option	Description
-A	L'option **-A** élimine l'impression des en-têtes de données.
-u	Avec l'option **-u** <*non d'utilisateur*> les résultats imprimés ne contiennent que les enregistrements de session concernant le nom d'utilisateur donné. Si un astérisque (*) est donné en tant que nom d'utilisateur, tous les utilisateurs sont répertoriés. Le résumé des informations n'est pas imprimé si cette option est spécifiée.

Exemples

- `racadm getssninfo`

Le tableau A-7 fournit un exemple de résultat de la commande **racadm getssninfo**.

Tableau A-7. Exemple de résultat de la sous-commande getssninfo

Utilisateur	Adresse IP	Type	Consoles
root	192.168.0.10	Telnet	Virtual KVM

- `racadm getssninfo -A`

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

- `racadm getssninfo -A -u *`

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

- `"bob" "143.166.174.19" "GUI" "NONE"`

---

getsysinfo

Le tableau A-8 décrit la sous-commande **racadm getsysinfo**.

Tableau A-8. getsysinfo

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

Synopsis

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

Description

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

Interfaces prises en charge

- RACADM locale

Entrées

Le tableau A-9 décrit les options de la sous-commande **getsysinfo**.

Tableau A-9. Options de la sous-commande getsysinfo

Option	Description
-d	Affiche les informations iDRAC.
-s	Affiche les informations sur le système
-w	Affiche les informations sur la surveillance.
-A	Élimine l'impression d'en-têtes/noms.

Résultat

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

Exemple de résultat

```
RAC Information:
RAC Date/Time            = Wed Aug 22 20:01:33 2007
Firmware Version         = 0.32
Firmware Build           = 13661
Last Firmware Update     = Mon Aug 20 08:09:36 2007

Hardware Version         = NA
Current IP Address       = 192.168.0.120
Current IP Gateway       = 192.168.0.1
Current IP Netmask       = 255.255.255.0
DHCP Enabled             = 1
MAC Address              = 00:14:22:18:cd:f9
```

```
Current DNS Server 1     = 10.32.60.4
Current DNS Server 2     = 10.32.60.5
DNS Servers from DHCP    = 1
Register DNS RAC Name    = 1
DNS RAC Name             = iDRAC-783932693338
Current DNS Domain       = us.dell.com

System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status             = OFF

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

Exemples

- `racadm getsysinfo -A -s`

  `"System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"`

- `racadm getsysinfo -w -s`

```
System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status            = ON


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 uniquement si Dell OpenManage est installé sur le serveur géré. Si OpenManage n'est pas installé sur le serveur géré, ces champs peuvent être vides ou inexacts.

---

getractime

Le tableau A-10 décrit la sous-commande **getractime**.

Tableau A-10. getractime

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

Synopsis

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

Description

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

Avec l'option **-d**, **getractime** affiche l'heure au format *yyyymmddhhmmss.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

20071208201542.000000
```

Interfaces prises en charge

- RACADM locale

---

setniccfg

Le tableau A-11 décrit la sous-commande **setniccfg**.

Tableau A-11. setniccfg

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

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 iDRAC.

- L'option **-d** active le protocole DHCP pour le NIC (la valeur par défaut est DHCP activé).
- 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
  ```

- L'option **-o** désactive le NIC entièrement. <*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

- RACADM locale

---

getniccfg

Le tableau A-12 décrit la sous-commande **getniccfg**.

Tableau A-12. getniccfg

Sous-commande	Définition
getniccfg	Affiche la configuration IP actuelle d'iDRAC.

Synopsis

```
racadm getniccfg
```

Description

La sous-commande **getniccfg** affiche les paramètres NIC actuels.

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

- RACADM locale

---

getsvctag

Le tableau A-13 décrit la sous-commande **getsvctag**.

Tableau A-13. 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

- RACADM locale

---

racreset

Le tableau A-14 décrit la sous-commande **racreset**.

Tableau A-14. racreset

Sous-commande	Définition
racreset	Réinitialise iDRAC.

AVIS : Lorsque vous émettez une sous-commande racreset, il faut jusqu'à une minute pour que iDRAC puisse retourner dans un état utilisable.

Synopsis

```
racadm racreset
```

Description

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

Exemples

- `racadm racreset`

  Démarre la séquence de redémarrage logicielle d'iDRAC.

Interfaces prises en charge

- RACADM locale

---

racresetcfg

Le tableau A-15 décrit la sous-commande **racresetcfg**.

Tableau A-15. 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

- RACADM locale

Description

La commande **racresetcfg** supprime toutes les entrées de propriétés de la base de données configurée par l'utilisateur. La base de données a des propriétés par défaut pour toutes les entrées utilisées pour restaurer les paramètres par défaut d'iDRAC.

AVIS : Cette commande supprime votre configuration iDRAC actuelle et réinitialise les paramètres par défaut d'iDRAC. Une fois la réinitialisation effectuée, le nom par défaut et le mot de passe sont respectivement **root** et **calvin**, et l'adresse IP est **192.168.0.120** plus le numéro de logement du serveur dans le châssis.

---

serveraction

Le tableau A-16 décrit la sous-commande **serveraction**.

Tableau A-16. serveraction

Sous-commande	Définition
serveraction	Exécute une réinitialisation ou une mise hors puis sous tension du serveur 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-17 décrit les options de contrôle de l'alimentation **serveraction**.

Tableau A-17. Options de la sous-commande serveraction

Chaîne de caractères	Définition
<*action***>**	Spécifie l'action. Les options de la chaîne de caractères<*action*> sont : • **powerdown** : met le serveur géré hors tension. • **powerup** : met le serveur géré sous tension. • **powercycle** : lance une opération de cycle d'alimentation sur le serveur 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. • **powerstatus** : affiche l'état actuel de l'alimentation du serveur (**Activé** ou **Désactivé**). • **hardreset** : effectue une opération de réinitialisation (redémarrage) sur le serveur 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

---

getraclog

Le tableau A-18 décrit la commande **racadm getraclog**.

Tableau A-18. getraclog

Commande	Définition
getraclog -i	Affiche le nombre d'entrées du journal iDRAC.

getraclog	Affiche les entrées du journal iDRAC.

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 iDRAC.

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

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

Tableau A-19. Options de la sous-commande getraclog

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

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 1er janvier et augmente jusqu'à ce que le serveur géré redémarre. Après le démarrage du serveur géré, l'heure système du serveur géré est utilisée pour l'horodatage.

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

- RACADM locale

---

clrraclog

Synopsis

```
racadm clrraclog
```

Description

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

---

getsel

Le tableau A-20 décrit la commande **getsel**.

Tableau A-20. getsel

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

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

Tableau A-21. Options de la sous-commande getsel

Option	Description
-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 du journal 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).

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

- RACADM locale

---

clrsel

Synopsis

```
racadm clrsel
```

Description

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

Interfaces prises en charge

- RACADM locale

---

gettracelog

Le tableau A-22 décrit la sous-commande **gettracelog**.

Tableau A-22. gettracelog

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

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 :

Tableau A-23. Options de la sous-commande gettracelog

Option	Description
-i	Affiche le nombre d'entrées du **journal de suivi iDRAC**.
-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 1er janvier et augmente jusqu'à ce que le système géré redémarre. Après le démarrage du système géré, l'heure système du système géré est utilisée pour l'horodatage.

Par exemple :

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

Interfaces prises en charge

- RACADM locale

---

sslcsrgen

Le tableau A-24 décrit la sous-commande **sslcsrgen**.

Tableau A-24. sslcsrgen

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

Synopsis

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

racadm sslcsrgen -s
```

Description

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

Options

Le tableau A-25 décrit les options de la sous-commande **sslcsrgen**.

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

Option	Description
-g	Crée une nouvelle RSC.
-s	Renvoie l'état du processus de création d'une RSC (génération en cours, active ou aucune).
-f	Spécifie le nom de fichier de l'emplacement, *<nom de fichier>*, où la RSC 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 RSC est générée et téléchargée dans le système de fichiers local comme **sslcsr** par défaut. L'option **-g** ne peut pas être utilisée avec l'option **-s** et l'option **-f** peut seulement être utilisée avec l'option **-g**.

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

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

REMARQUE : Avant de pouvoir générer une RSC, les champs de la RSC 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

- RACADM locale

---

sslcertupload

Le tableau A-26 décrit la sous-commande **sslcertupload**.

Tableau A-26. sslcertupload

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

Synopsis

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

Options

Le tableau A-27 décrit les options de la sous-commande **sslcertupload**.

Tableau A-27. Options de la sous-commande sslcertupload

Option	Description
-t	Spécifie le type de certificat à téléverser, 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 téléverser Si le fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.

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

Exemple

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

Interfaces prises en charge

- RACADM locale

---

sslcertdownload

Le tableau A-28 décrit la sous-commande **sslcertdownload**.

Tableau A-28. sslcertdownload

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

Synopsis

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

Options

Le tableau A-29 décrit les options de la sous-commande **sslcertdownload**.

Tableau A-29. Options de la sous-commande sslcertdownload

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

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

Exemple

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

Interfaces prises en charge

- RACADM locale

---

sslcertview

Le tableau A-30 décrit la sous-commande **sslcertview**.

Tableau A-30. sslcertview

Sous-commande	Description
sslcertview	Affiche le serveur SSL ou le certificat d'une autorité de certification qui existe sur iDRAC.

Synopsis

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

Options

Le tableau A-31 décrit les options de la sous-commande **sslcertview**.

Tableau A-31. 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)          : iDRAC 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)           : iDRAC 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
iDRAC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces prises en charge

- RACADM locale

---

testemail

Le tableau A-32 décrit la sous-commande **testemail**.

Tableau A-32. Configuration de testemail

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

Synopsis

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

Description

Envoie un e-mail test à partir d' iDRAC vers une destination spécifiée.

Avant d'exécuter la commande testemail, assurez-vous que l'index spécifié dans le groupe RACADM **cfgEmailAlert** est activé et configuré correctement. Le tableau A-33 fournit un exemple de commandes pour le groupe **cfgEmailAlert**.

Tableau A-33. 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 cfgRhostsSmtpServerIpAddr -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-34 décrit les options de la sous-commande **testemail**.

Tableau A-34. Option de la sous-commande testemail

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

Résultat

Aucun.

Interfaces prises en charge

- RACADM locale

---

testtrap

Le tableau A-35 décrit la sous-commande **testtrap**.

Tableau A-35. testtrap

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

Synopsis

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

Description

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

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

Le tableau A-36 fournit une liste et les commandes associées pour le groupe **cfgIpmiPet**.

Tableau A-36. Commandes d'alerte par e-mail cfg

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-37 décrit les options de la sous-commande **testtrap**.

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

Option	Description

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

Interfaces prises en charge

- RACADM locale

---

vmdisconnect

Le tableau A-38 décrit la sous-commande **vmdisconnect**.

Tableau A-38. vmdisconnect

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

Synopsis

```
racadm vmdisconnect
```

Description

La sous-commande **vmdisconnect** permet à un utilisateur de fermer la session du média virtuel d'un autre utilisateur. Une fois la session fermée, l'interface Web reflétera l'état de la connexion appropriée. Cette sous-commande n'est disponible que si vous utilisez un utilitaire RACADM local.

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

Interfaces prises en charge

- RACADM locale

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 iDRAC

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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

Utilisez les numéros des groupes et des objets avec l'utilitaire RACADM pour configurer iDRAC. 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 :

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

Ce groupe contient des paramètres d'affichage pour les informations sur les spécifications du contrôleur iDRAC 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

Integrated Dell Remote Access Controller

Description

Une chaîne de texte qui identifie 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 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

iDRAC

Description

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

idRacType (lecture seule)

Valeur par défaut

8

Description

Identifie le type de Remote Access Controller comme iDRAC.

---

cfgLanNetworking

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

Une seule instance du groupe est autorisée. Tous les objets de ce groupe nécessitent une réinitialisation du NIC iDRAC, ce qui interrompra peut-être brièvement la connectivité. Les objets qui modifient les paramètres de l'adresse IP du NIC iDRAC 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)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgDNSDomainName (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères ASCII au maximum. Au moins une 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 (FAUX).

cfgDNSRacName (lecture/écriture)

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

cfgDNSRegisterRac (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Enregistre le nom iDRAC sur le serveur DNS.

cfgDNSServersFromDHCP (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

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)

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** (FAUX).

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

cfgDNSServer2 (lecture/écriture)

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 (FAUX).

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

cfgNicEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgNicIpAddress (lecture/écriture)

REMARQUE : Ce paramètre est uniquement configurable 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.*n*

où *n* est 120 plus le numéro de logement du serveur.

Description

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

cfgNicNetmask (lecture/écriture)

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

Valeurs valides

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

Valeur par défaut

255.255.255.0

Description

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

cfgNicGateway (lecture/écriture)

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

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 RAC. Cette propriété n'est valide que si **cfgNicUseDhcp** est défini sur **0** (FAUX).

cfgNicUseDhcp (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgNicMacAddress (lecture seule)

Valeurs valides

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

Valeur par défaut

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

Description

Adresse MAC du NIC iDRAC.

---

cfgUserAdmin

Ce groupe fournit des informations de configuration sur les utilisateurs qui ont le droit d'accéder à 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)

Valeurs valides

2 (**utilisateur**)

3 (opérateur)

4 (**administrateur**)

15 (**pas d'accès**)

Valeur par défaut

4 (utilisateur 2)

15 (tous les autres)

Description

Privilège maximum sur le canal LAN IPMI.

cfgUserAdminPrivilege (lecture/écriture)

Valeurs valides

De 0x00000000 à 0x000001ff

Valeur par défaut

0x00000000

Description

Cette propriété spécifie les privilèges basés sur le rôle qui sont autorisés pour l'utilisateur. La valeur est représentée comme un masque binaire qui autorise n'importe quelle combinaison de valeurs de privilège. Le tableau B-1 décrit les valeurs binaires des droits d'utilisateur pouvant être combinées pour créer des masques binaires.

Tableau B-1. Masques binaires des droits d'utilisateur

Droit d'utilisateur	Masque binaire de privilège
Ouvrir une session iDRAC	0x0000001

Configuration d'iDRAC	0x0000002
Configuration des utilisateurs	0x0000004
Effacer les journaux	0x0000008
Exécution des commandes de contrôle du serveur	0x0000010
Accès à la redirection de console	0x0000020
Accès au média virtuel	0x0000040
Tester les alertes	0x0000080
Exécution des commandes de débogage	0x0000100

Exemples

Le tableau B-2 fournit des exemples de masques binaires pour les utilisateurs avec un ou plusieurs privilèges.

Tableau B-2. 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 à iDRAC.	0x00000000
L'utilisateur peut uniquement se connecter à iDRAC et afficher les informations de configuration iDRAC et du serveur.	0x00000001
L'utilisateur peut se connecter à iDRAC et modifier la configuration.	0x00000001 + 0x00000002 = 0x00000003
L'utilisateur peut se connecter à RAC, accéder au média virtuel et à la redirection de console.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lecture/écriture)

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 parmi les noms d'utilisateur.

cfgUserAdminPassword (lecture seule)

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

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive un utilisateur.

cfgUserAdminSolEnable

Valeurs valides

1 (VRAI)

0 (FAUX)

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 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 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgEmailAlertAddress

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

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 à iDRAC.

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

cfgSsnMgtConsRedirMaxSessions (lecture/écriture)

Valeurs valides

1 – 2

Valeur par défaut

2

Description

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

cfgSsnMgtWebserverTimeout (lecture/écriture)

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)

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.

cfgSsnMgtTelnetIdleTimeout (lecture/écriture)

Valeurs valides

0 (pas de délai d'attente)

60 – 1920

Valeur par défaut

300

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 uniquement 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)
```

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

---

cfgSerial

Ce groupe contient les paramètres de configuration des services iDRAC.

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

cfgSerialSshEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

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

cfgSerialTelnetEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

---

cfgRacTuning

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

cfgRacTuneHttpPort (lecture/écriture)

Valeurs valides

10 – 65535

Valeur par défaut

80

Description

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

cfgRacTuneHttpsPort (lecture/écriture)

Valeurs valides

10 – 65535

Valeur par défaut

443

Description

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

cfgRacTuneIpRangeEnable

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgRacTuneIpRangeAddr

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

Valeurs valides

Valeurs de masque IP standard avec bits justifiés à gauche

Valeur par défaut

255.255.255.0

Description

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

cfgRacTuneIpBlkEnable

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgRacTuneIpBlkFailCount

Valeurs valides

2 – 16

Valeur par défaut

5

Description

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

cfgRacTuneIpBlkFailWindow

Valeurs valides

10 – 65535

Valeur par défaut

60

Description

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

cfgRacTuneIpBlkPenaltyTime

Valeurs valides

10 – 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)

Valeurs valides

1 – 65535

Valeur par défaut

22

Description

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

cfgRacTuneTelnetPort (lecture/écriture)

Valeurs valides

1 – 65535

Valeur par défaut

23

Description

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

cfgRacTuneConRedirEncryptEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Encrypte la vidéo dans une session de redirection de console.

cfgRacTuneConRedirPort (lecture/écriture)

Valeurs valides

1 – 65535

Valeur par défaut

5900

Description

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

cfgRacTuneConRedirVideoPort (lecture/écriture)

Valeurs valides

1 – 65535

Valeur par défaut

5901

Description

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

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

cfgRacTuneAsrEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

0

Description

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

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

cfgRacTuneWebserverEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

1

Description

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

cfgRacTuneLocalServerVideo (lecture/écriture)

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)

Valeurs valides

Chaîne. Longueur maximale = 255.

Valeur par défaut

""

Description

Le nom d'hôte du serveur géré.

ifcRacMnOsOsName (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 255.

Valeur par défaut

""

Description

Nom du système d'exploitation du serveur géré.

---

cfgRacSecurity

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

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)

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

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

cfgSecCsrOrganizationName (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

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

cfgSecCsrOrganizationUnit (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

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

cfgSecCsrLocalityName (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie la ville (L) de la RSC.

cfgSecCsrStateName (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le nom d'état (S) de la RSC.

cfgSecCsrCountryCode (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 2.

Valeur par défaut

""

Description

Spécifie l'indicatif du pays (CC) de la RSC

cfgSecCsrEmailAddr (lecture/écriture)

Valeurs valides

Chaîne. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie l'adresse e-mail de la RSC.

cfgSecCsrKeySize (lecture/écriture)

Valeurs valides

1024

2048

4096

Valeur par défaut

1024

Description

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

---

cfgRacVirtual

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

cfgVirMediaAttached (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

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

Valeurs valides

1 – 65535

Valeur par défaut

3668

Description

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

cfgVirAtapiSrvPortSsl (lecture/écriture)

Valeurs valides

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

Valeur par défaut

3670

Description

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

cfgVirMediaBootOnce (lecture/écriture)

Valeurs valides

1 (activé)

0 (désactivé)

Valeur par défaut

0

Description

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

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Lorsqu'il est défini sur 0, le lecteur de disquette virtuel est reconnu comme un disque amovible par les systèmes d'exploitation Windows. Les systèmes d'exploitation Windows attribuent 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 iDRAC.

cfgADRacDomain (lecture/écriture)

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 DRAC.

cfgADRacName (lecture/écriture)

Valeurs valides

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

Valeur par défaut

""

Description

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

cfgADEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

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

cfgADAuthTimeout (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez disposer de l'autorisation de **configurer iDRAC**.

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)

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.

cfgADSpecifyServerEnable (lecture/écriture)

Valeurs valides

1 ou 0 (vrai ou faux)

Valeur par défaut

0

Description

1 (vrai) vous permet d'indiquer un serveur LDAP ou un serveur de catalogue global. 0 (faux) désactive cette option.

cfgADDomainController (lecture/écriture)

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADGlobalCatalog (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADType (lecture/écriture)

Valeurs valides

1 = active Active Directory avec le schéma étendu.

2 = active Active Directory avec le schéma standard.

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 d'Active Directory.

cfgSSADRoleGroupIndex (lecture seule)

Valeurs valides

Entier de 1 à 5.

Description

Index du groupe de rôles enregistré dans Active Directory.

cfgSSADRoleGroupName (lecture/écriture)

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)

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)

Valeurs valides

De **0x00000000** à **0x000001ff**

Valeur par défaut

(aucune)

Description

Utilisez les numéros de masques binaires du tableau B-3 pour définir des privilèges d'autorisation basées sur un groupe de rôles.

Tableau B-3. Masques binaires pour des privilèges de groupes de rôles

Privilège de groupes de rôles	Masque binaire
Ouvrir une session iDRAC	0x00000001
Configuration d'iDRAC	0x00000002
Configuration des utilisateurs	0x00000004
Effacer les journaux	0x00000008
Exécution des commandes de contrôle du serveur	0x00000010
Accès à la redirection de console	0x00000020
Accès au média virtuel	0x00000040
Tester les alertes	0x00000080
Exécution des commandes de débogage	0x00000100

---

cfgIpmiSol

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

cfgIpmiSolEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

1

Description

Active ou désactive les communications série sur le LAN.

cfgIpmiSolBaudRate (lecture/écriture)

Valeurs valides

19200, 57600, 115200

Valeur par défaut

115200

Description

Débit en bauds pour la communication série sur le LAN.

cfgIpmiSolMinPrivilege (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

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

cfgIpmiSolAccumulateInterval (lecture/écriture)

Valeurs valides

1 à 255.

Valeur par défaut

10

Description

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

cfgIpmiSolSendThreshold (lecture/écriture)

Valeurs valides

1 – 255

Valeur par défaut

255

Description

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

---

cfgIpmiLan

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

cfgIpmiLanEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

0

Description

Active ou désactive l'interface IPMI sur le LAN.

cfgIpmiLanPrivLimit (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

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

cfgIpmiLanAlertEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

0

Description

Active ou désactive l'ensemble des alertes par e-mail. Cette propriété remplace toutes les propriétés individuelles d'activation et de désactivation des alertes par e-mail.

cfgIpmiEncryptionKey (lecture/écriture)

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)

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 serveur 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)

Valeurs valides

0 (aucun)

1 (mise hors tension)

2 (réinitialisation)

3 (cycle d'alimentation)

Valeur par défaut

0

Description

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

cfgIpmiPefEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

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 serveur géré.

cfgIpmiPetIndex (lecture/écriture)

Valeurs valides

1 – 4

Valeur par défaut

Valeur d'index appropriée.

Description

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

cfgIpmiPetAlertDestIpAddr (lecture/écriture)

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 serveur géré.

cfgIpmiPetAlertEnable (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

1

Description

Active ou désactive une interruption spécifique.

Retour à la page du sommaire

Retour à la page du sommaire

Équivalences RACADM et SM-CLP

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Le tableau C-1 répertorie les groupes et objets RACADM et, le cas échéant, les emplacements équivalents SM-SLP dans l'adressage SM-CLP.

Tableau C-1. Équivalences RACADM et SM-CLP

Groupe RACADM	SM-CLP	Description
idRacInfo		
idRacName		Chaîne de 15 caractères ASCII au maximum. Par défaut : **iDRAC**.
idRacProductInfo		Chaîne de 63 caractères ASCII au maximum. Par défaut : **Integrated Dell Remote Access Controller**.
idRacDescriptionInfo		Chaîne de 255 caractères ASCII au maximum. Par défaut : **ce composant système fournit aux serveurs Dell PowerEdge un ensemble complet de fonctions de gestion à distance.**
idRacVersionInfo		Chaîne de 63 caractères ASCII au maximum. Par défaut : **1**
idRacBuildInfo		Chaîne de 16 caractères ASCII au maximum.
idRacType		Par défaut : **8**
cfgActiveDirectory	**/system1/sp1/oemdell_adservice1**	
cfgADEnable	enablestate	0 pour désactiver, 1 pour activer. Par défaut : **0**
cfgADRacName	oemdell_adracname	Chaîne de pas plus de 254 caractères.
cfgADRacDomain	oemdell_adracdomain	Chaîne de pas plus de 254 caractères.
cfgADRootDomain	oemdell_adrootdomain	Chaîne de pas plus de 254 caractères.
cfgADAuthTimeout	oemdell_timeout	15 à 300 secondes. Par défaut : **120**
cfgADType	oemdell_schematype	1 pour le schéma standard, 2 pour le schéma étendu. Par défaut : **1**
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1** *through* **/system1/sp1/group5**	RACADM : numéro d'index de groupe de 1 à 5. SM-CLP : sélectionné avec le chemin de l'adresse
cfgSSADRoleGroupName	oemdell_groupname	Chaîne de pas plus de 254 caractères.
cfgSSADRoleGroupDomain	oemdell_groupdomain	Chaîne de pas plus de 254 caractères.
cfgSSADRoleGroupPrivilege	oemdell_grouppprivilege	Masque binaire avec des valeurs entre 0x00000000 et 0x000001ff.
cfgLanNetworking	**/system1/sp1/enetport1**	
cfgNicMacAddress	macaddress	Adresse MAC de l'interface. Non modifiable.
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicEnable	oemdell_nicenable	0 pour désactiver le NIC, 1 pour l'activer. Par défaut : **0**
cfgNicUseDHCP	oemdell_usedhcp	0 pour configurer les adresses réseau statiques, 1 pour utiliser DHCP. Par défaut : **0**
cfgNicIpAddress	ipaddress	Adresse IP d'iDRAC. Par défaut : **192.168.0.120** plus le numéro de logement du serveur.
cfgNicNetmask	subnetmask	Masque de sous-réseau du réseau iDRAC. Par défaut : **255.255.255.0**
	committed	Lorsque les valeurs d'un groupe changent, la valeur de **committed** est définie sur 0 pour indiquer que les nouvelles valeurs n'ont pas été enregistrées. Définissez la valeur sur 1 pour enregistrer la nouvelle configuration. Par défaut : **1**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdell_dnsdomainname	Chaîne de 254 caractères ASCII au maximum. Au moins un caractère doit être une lettre.
cfgDNSDomainNameFromDHCP	oemdell_domainnamefromdhcp	À définir sur 1 pour obtenir le nom de domaine auprès de DHCP. Par défaut : **0**
cfgDNSRacName	oemdell_dnsracname	Chaîne de 63 caractères ASCII au maximum. Au moins un caractère doit être une

		lettre. Par défaut : **iDRAC-** *plus le numéro de service Dell*.
cfgDNSRegisterRac	oemdell_dnsregisterrac	À difinir sur 1 pour enregistrer le nom iDRAC sur DNS. Par défaut : **0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	ã définir sur 1 pour obtenir les adresses du serveur DNS auprès de DHCP. Par défaut : **0**
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	Chaîne de caractères représentant l'adresse IP d'un serveur DNS.
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer2	dnsserveraddresses2	Chaîne de caractères représentant l'adresse IP d'un serveur DNS.
	/server1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	Chaîne de caractères représentant l'adresse IP de la passerelle par défaut. Par défaut : **192.168.0.1**
cfgRacVirtual	**/server1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	À définir sur 1 pour activer l'émulation de disquette. Par défaut : **0**
cfgVirMediaAttached	enabledstate	À définir sur 1 (RACADM)/VMEDIA_ATTACH (SM-CLP)pour connecter un média. Par défaut : 1 (RACADM)/VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdell_singleboot	À définir sur 1 pour lancer le prochain démarrage à partir du média sélectionné. Par défaut **0**.
	/server1/sp1/oemdell_vmservice1/tcpendpt1	
	oemdell_sslenabled	À définir sur 1 si SSL est activé pour le premier média virtuel, 0 si ce n'est pas le cas. Non modifiable.
cfgVirAtapiSvrPort	portnumber	Port à utiliser pour le premier média virtuel. Par défaut : **3668**
	/server1/sp1/oemdell_vmservice1/tcendpt2	
	oemdell_sslenabled	À définir sur 1 si SSL est activé pour le deuxième média virtuel, 0 si ce n'est pas le cas. Non modifiable.
cfgVirAtapiSvrPortSsl	portnumber	Port à utiliser pour le deuxième média virtuel. Par défaut : **3670**
cfgUserAdmin	**/server1/sp1/oemdell_vmservice1/tcpendpt2**	
cfgUserAdminEnable	enabledstate	À définir sur 1 pour activer un utilisateur. Par défaut : **0**
cfgUserAdminIndex	userid	Index utilisateur de 1 à 16.
cfgUserAdminIpmiLanPrivilege	oemdell_ipmilanprivileges	2 (utilisateur), 3 (opérateur), 4 (administrateur) ou 15 (pas d'accès). Par défaut : **4**
cfgUserAdminPassword	password	Chaîne de 20 caractères ASCII au maximum.
cfgUserAdminPrivilege	oemdell_extendedprivileges	Masque binaire entre 0x00000000 et 0x000001ff. Par défaut : **0x00000000**
cfgUserAdminSolEnable	solenabled	À définir sur 1 pour permettre à un utilisateur d'utiliser les communications série sur le LAN. Par défaut : **0**
cfgUserAdminUserName	username	Chaîne de pas plus de 16 caractères.
cfgEmailAlert		
cfgEmailAlertAddress		Adresse e-mail de destination ; pas plus de 64 caractères.
cfgEmailAlertCustomMsg		Message e-mail à envoyer ; pas plus de 32 caractères.
cfgEmailAlertEnable		À définir sur 1 pour activer une alerte par e-mail. Par défaut : **0**
cfgEmailAlertIndex		Index de l'instance de l'alerte par e-mail. Chiffre de 1 à 4.
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		Nombre de sessions de Redirection de console simultannées autorisées (1 ou 2). Par défaut : **2**
cfgSsnMgtSshIdleTimeout		Nombre de secondes d'inactivité avant l'expiration d'une session SSH. 0 pour désactiver le délai d'attente ou entre 60 et 1920 secondes. Par défaut : **300**
cfgSsnMgtTelnetIdleTimeout		Nombre de secondes d'inactivité avant l'expiration d'une session Telnet. 0 pour désactiver le délai d'attente ou entre 60 et 1920 secondes. Par défaut : **300**
cfgSsnMgtWebserverTimeout		Nombre de secondes d'inactivité avant l'expiration d'une session d'interface

		Web. Entre 60 et 1920 secondes. Par défaut : **300**
cfgRacTuning		
cfgRacTuneConRedirEnable		À définir sur 1 pour activer la redirection de console, sur 0 pour la désactiver. Par défaut :**1**
cfgRacTuneConRedirEncrypt Enable		À définir sur 1 pour activer le cryptage du trafic réseau de la redirection de console, sur 0 pour le désactiver. Par défaut : **1**
cfgRacTuneConRedirPort		Port à utiliser pour la redirection de console. Par défaut : **5900**
cfgRacTuneConRedirVideoPort		Port à utiliser pour la redirection vidéo de la console. Par défaut : **5901**
cfgRacTuneHttpPort		Port à utiliser pour l'adresse HTTP de l'interface Web. Par défaut : **80**
cfgRacTuneHttpsPort		Port à utiliser pour l'adresse HTTPS sécurisée de l'interface Web. Par défaut : **443**
cfgRacTuneIpBlkEnable		À définir sur 1 pour activer le blocage IP. Par défaut : **0**
cfgRacTuneIPBlkFailCount		Nombre d'échecs de tentatives d'ouverture de session à compter avant d'utiliser le blocage IP (entre 2 et 16). Par défaut : **5**
cfgRacTuneIpBlkFailWindow		Délai en secondes du compte des échecs de tentatives d'ouverture de session (entre 10 et 65 535). Par défaut : **60**
cfgRacTuneIpBlkPenaltyTime		Délai en secondes pendant lequel une adresse IP bloquée reste bloquée (entre 10 et 65 535). Par défaut : **300**
cfgRacTuneIpRangeAddr		Adresse IP de base du filtre des plages d'adresses IP. Par défaut : **192.168.0.1**
cfgRacTuneIpRangeEnable		À définir sur 1 pour activer le filtrage des plages d'adresses IP. Par défaut : 0
cfgRacTuneIpRangeMask		Masque binaire appliqué à l'adresse de base permettant de sélectionner des adresses IP valides. Par défaut : **255.255.255.0**
cfgRacTuneLocalServerVideo		À définir sur 1 pour activer la console iKVM locale. Par défaut : **1**
cfgRacTuneSshPort		Port à utiliser pour le service SSH. Par défaut : **22**
cfgRacTuneTelnetPort		Port à utiliser pour le service Telnet. Par défaut : **23**
cfgRacTuneWebserverEnable		À définir sur 1 pour activer l'interface Web iDRAC. Par défaut : **1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		Nom d'hôte du serveur géré. Chaîne de pas plus de 255 caractères.
ifcRacMnOsOsName		Nom du système d'exploitation du serveur géré. Chaîne de pas plus de 255 caractères.
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Nom de domaine d'Active Directory. Chaîne de pas plus de 254 caractères.
cfgRacSecCsrCountryCode	oemdell_countrycode	Code de pays d'Active Directory. 2 caractères.
cfgRacSecCsrEmailAddr	oemdell_emailaddress	Adresse e-mail à utiliser pour la requête de signature de certificat. Chaîne de pas plus de 254 caractères.
cfgRacSecCsrKeySize	oemdell_keysize	Longueur de la clé de cryptage (512, 1024 ou 2048). Par défaut : **1024**.
cfgRacSecCsrLocalityName	oemdell_localityname	Nom de la ville où se trouve Active Directory. Chaîne de pas plus de 254 caractères.
cfgRacSecCsrOrganizationName	organizationname	Nom de la compagnie possédant Active Directory. Chaîne de pas plus de 254 caractères.
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Nom du service de la compagnie possédant Active Directory. Chaîne de pas plus de 254 caractères.
cfgRacSecCsrStateName	oemdell_statename	Nom de l'état ou de la région où se trouve Activity Directory. Chaîne de pas plus de 254 caractères.
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Nombre maximal de millisecondes à attendre avant d'envoyer un paquet partiel de communications série sur le LAN (entre 1 et 255). Par défaut : **10**
cfgIpmiSolBaudRate		Débit en bauds à utiliser pour les communications série sur le LAN (19 200, 57 600, 115 200). Par défaut : **115200**
cfgIpmiSolEnable		À définir sur 1 pour activer les communications série sur le LAN. Par défaut : **0**
cfgIpmiSolSendThreshold		Nombre maximal de caractères à reccueillir avant d'envoyer des données SOL (entre 1 et 255). Par défaut : **255**
cfgIpmiSolMinPrivilege		Minimum de privilèges requis pour utiliser SOL. 2 (utilisateur), 3 (opérateur), ou 4 (administrateur). Par défaut : **4**
cfgIpmiLan		
cfgIpmiEncryptionKey		Chaîne de caractères de 0 à 40 chiffres hexadécimaux. Par défaut : **00000000000000000000000000000000000000000000**
cfgIpmiLanAlertEnable		À définir sur 1 pour activer les alertes LAN IPMI. Par défaut : **0**
cfgIpmiLanEnable		À définir sur 1 pour activer l'interface IPMI sur le LAN. Par défaut : **0**
cfgIpmiPetCommunityName		Chaîne de pas plus de 18 caractères. Par défaut : **public**

cfgIpmiPef		
cfgIpmiPefAction		Action à prendre lors de la détection d'un événement. 0 (aucune), 1 (mise hors tension), 2 (réinitialisation), 3 (cycle d'alimentation). Par défaut : **0**
cfgIpmiPefEnable		À définir sur 1 pour activer le filtrage des événements sur plateforme. Par défaut : **0**
cfgIpmiPefIndex		Nombre d'indexage du filtre d'événements sur plateforme (entre 1 et 17).
cfgIpmiPefName		Nom de l'événement sur plateforme, une chaîne de pas plus de 254 caractères. Non modifiable.
cfgIpmiPet		
cfgIpmiPetAlertDestIpAddr		Adresse IP du récepteurs de l'interruption d'événement sur plateforme. Par défaut : **0.0.0.0**
cfgIpmiPetAlertEnable		À définir sur 1 pour activer l'interruption d'événement sur plateforme. Par défaut : **1**
cfgIpmiPetIndex		Chiffre d'indexage (entre 1 et 4) de l'interruption d'événement sur plateforme.

Retour à la page du sommaire

Retour à la page du sommaire

Présentation d'iDRAC

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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

iDRAC utilise un microprocesseur « système sur une puce » intégré pour le système de surveillance/contrôle distant. iDRAC coexiste sur la carte système avec le serveur PowerEdge géré. Le système d'exploitation du serveur, qu'il s'agisse de Microsoft® Windows® ou de Linux, se charge de l'exécution des applications ; iDRAC se charge, quant à lui, de la surveillance et de la gestion de l'environnement du serveur et de l'état hors du système d'exploitation.

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

Les serveurs gérés sont installés dans une enceinte (châssis) du système Dell M1000-e avec des blocs d'alimentation modulaires, des ventilateurs et un CMC (Chassis Management Controller). CMC surveille et gère tous les composants installés dans le châssis. Des CMC redondants peuvent être ajoutés pour assurer un basculement à chaud si le CMC principal échoue. Le châssis permet d'accéder aux iDRAC via son écran LCD, les connexions de console locale et son interface Web.

Toutes les connexions réseau à iDRAC s'effectuent via l'interface réseau CMC (port de connexion CMC RJ45 nommé « GB1 »). CMC achemine le trafic vers les iDRAC sur ses serveurs par le biais d'un réseau privé interne. Ce réseau de gestion privé se trouve hors du chemin des données du serveur et hors du contrôle du système d'exploitation, autrement dit *hors bande*. Les interfaces réseau *intrabandes* des serveurs gérés sont accessibles via les modules d'E/S (IOM) installés dans le châssis.

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

Fonctionnalités de gestion iDRAC

iDRAC intègre les fonctionnalités de gestion suivantes :

- Enregistrement de système de noms de domaine dynamique (DDNS)
- Gestion du système distant et surveillance via une interface Web, l'interface de ligne de commande RACADM locale via la redirection de console et la ligne de commande SM-CLP via une connexion Telnet/SSH
- Prise en charge de l'authentification Microsoft Active Directory® : centralise les références utilisateur et les mots de passe iDRAC dans Active Directory à l'aide du schéma standard ou d'un schéma étendu
- Redirection de console : fournit les fonctions de clavier, vidéo et souris à distance
- Média virtuel : permet à un serveur géré d'accéder à un lecteur de média local sur la station de gestion ou aux images de CD/DVD ISO sur un partage réseau
- Surveillance : permet d'accéder aux informations sur le système et à la condition des composants
- Accès aux journaux système : permet d'accéder au journal des événements système, au journal iDRAC et à l'écran de la dernière panne du système fermé subitement ou sans réponse qui est indépendant de l'état du système d'exploitation
- Intégration du logiciel Dell OpenManage™ : vous permet de lancer l'interface Web iDRAC à partir de Dell OpenManage Server Administrator ou d'IT Assistant
- Alerte iDRAC : vous avertit des problèmes de nœud géré potentiels via un message électronique ou une interruption SNMP
- Gestion de l'alimentation à distance : fournit des fonctionnalités de gestion de l'alimentation à distance, comme l'arrêt et la réinitialisation, à partir d'une console de gestion
- Prise en charge d'interface de gestion de plateforme intelligente (IPMI)
- Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système à distance via l'interface Web
- Gestion de la sécurité de niveau mot de passe : empêche tout accès non autorisé à un système distant
- Autorisation basée sur le rôle : permet d'attribuer des droits pour diverses tâches de gestion de systèmes

---

Fonctionnalités de sécurité iDRAC

iDRAC intègre les fonctionnalités de sécurité suivantes :

- Authentification des utilisateurs via Microsoft Active Directory (en option) ou via les références utilisateur et les mots de passe stockés sur le matériel
- Autorité basée sur le rôle, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- Configuration des références utilisateur et des mots de passe via l'interface Web ou SM-CLP

- SM-CLP et interfaces Web prenant en charge le cryptage SSL 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté)
- Configuration du délai d'expiration de la session (en secondes) via l'interface Web ou SM-CLP
- Ports IP configurables (si applicable)

  REMARQUE : Telnet ne prend pas en charge le cryptage SSL.

- Secure Shell (SSH) qui utilise une couche de transport cryptée pour une sécurité plus élevée
- Nombre 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
- Plage d'adresses IP limitée pour les clients se connectant à iDRAC

Plateformes prises en charge

iDRAC prend en charge les systèmes PowerEdge suivants dans l'enceinte du système Dell PowerEdge M1000-e :

- PowerEdge M600
- PowerEdge M605

Consultez le fichier « Lisez-moi » iDRAC et le *Guide de compatibilité de Dell PowerEdge* qui se trouvent sur le site Web de support de Dell à l'adresse **support.dell.com** pour connaître les dernières plateformes prises en charge.

Systèmes d'exploitation pris en charge

Le tableau 1-1 répertorie les systèmes d'exploitation qui prennent en charge iDRAC.

Consultez le *Guide de compatibilité de Dell OpenManage Server Administrator* qui se trouve sur le site Web de support de Dell à l'adresse **support.dell.com** pour les dernières informations.

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

Gamme de systèmes d'exploitation	Système d'exploitation
Microsoft Windows	Microsoft® Windows Server® 2003 R2 éditions Standard et Enterprise (32 bits x86) avec SP2 Microsoft Windows Server 2003 éditions Web, Standard et Enterprise (32 bits x86) avec SP2 Microsoft Windows Server 2003 éditions Standard et Enterprise (x64) avec SP2 Microsoft Windows Storage Server 2003 R2 éditions Express, Workgroup, Standard et Enterprise x64 Microsoft Windows Vista® éditions Gold Business et Enterprise Microsoft Windows Server 2008 éditions Web, Standard et Enterprise (32 bits x86) Microsoft Windows Server 2008 éditions Web, Standard, Enterprise et DataCenter (x64) **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, voir l'article 903220 sur le site Web de support de Microsoft à l'adresse **support.microsoft.com/kb/903220**.
Red Hat® Linux®	Enterprise Linux WS, ES et AS, version 3 (x86 et x86_64) Enterprise Linux WS, ES et AS, version 4 (x86 et x86_64). Enterprise Linux 5 (x86 et x86-64).
SUSE® Linux	Enterprise Server 9 avec mises à jour 2 et 3 (x86_64) Enterprise Server 10 (Gold) (x86_64)

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 génère des résultats inattendus ou des pannes.

Le tableau 1-2 répertorie les navigateurs Web pris en charge en tant que clients iDRAC.

Voir le fichier « Lisez-moi » iDRAC et le *Guide de compatibilité de Dell OpenManage Server Administrator* qui se trouvent sur le site Web de support de Dell à

l'adresse **support.dell.com** pour les dernières informations.

Tableau 1-2. Navigateurs Web pris en charge

Système d'exploitation	Navigateur Web pris en charge
Windows	Internet Explorer 6.0 (32 bits) avec Service Pack 2 (SP2) uniquement pour Windows XP et Windows 2003 R2 SP2. Internet Explorer 7.0 pour Windows Vista, Windows XP et Windows 2003 R2 SP2 uniquement.
Linux	Mozilla Firefox 1.5 (32 bits) uniquement sur SUSE Linux (version 10). Mozilla Firefox 2.0 (32 bits).

Connexions d'accès à distance prises en charge

Le tableau 1-3 répertorie les fonctionnalités de connexion.

Tableau 1-3. Connexions d'accès à distance prises en charge

Connexion	Fonctionnalités
NIC iDRAC	• Ethernet 10 Mbits/s /100 Mbits/s /1 Gbits/s via port Ethernet Go CMC • Prise en charge de DHCP • Interruptions SNMP et notifications d'événements par e-mail • Prise en charge de l'environnement de commande SM-CLP (Telnet ou SSH) pour les opérations telles que la configuration iDRAC, le démarrage système, la réinitialisation, la mise sous tension et les commandes d'arrêt • Prise en charge des utilitaires IPMI, tels que ipmitool et ipmishell

---

Ports iDRAC

Le tableau 1-4 répertorie les ports sur lesquels iDRAC écoute les connexions. Le tableau 1-5 identifie les ports qu'iDRAC utilise comme client. Ces informations sont requises pour ouvrir des pare-feu pour pouvoir accéder à distance à iDRAC.

Tableau 1-4. Ports d'écoute du serveur iDRAC

Numéro de port	Fonctionnalité
22*	Protocole Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668*, 3669*	Service de média virtuel
3770*, 3771*	Service sécurisé de média virtuel
5900*	Clavier/souris de redirection de console
5901*	Vidéo de redirection de console
* Port configurable	

Tableau 1-5. Ports clients iDRAC

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)

Autres documents utiles

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

- L'aide en ligne d'iDRAC fournit des informations sur l'utilisation de l'interface Web.
- Le *Guide d'utilisation du micrologiciel Dell CMC, version 1.0* contient des informations sur l'utilisation du contrôleur qui gère tous les modules dans le châssis contenant votre serveur PowerEdge.
- 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.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator* contient des informations sur l'installation et l'utilisation de Server Administrator.
- Le *Guide d'utilisation des progiciels Dell Update Packages* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Packages dans le 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 iDRAC est installé :

- 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.
- Le *Guide d'installation du rack* et les *Instructions d'installation en rack* fournis avec votre rack décrivent comment installer votre système dans un rack.
- Le *Guide de démarrage rapide* présente les fonctionnalités du système, la configuration du système et les spécifications techniques.
- 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.
- La documentation du logiciel de gestion de systèmes décrit les fonctionnalités, les spécifications, l'installation et l'utilisation de base du logiciel.
- La documentation du système d'exploitation décrit comment installer (au besoin), configurer et utiliser le logiciel du système d'exploitation.
- La documentation des composants que vous avez achetés à part fournit des informations pour configurer et installer ces options.
- 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.

- 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

Configuration d'iDRAC

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Cette section contient des informations sur la façon d'accéder à iDRAC et de configurer votre environnement de gestion pour utiliser iDRAC.

Avant de commencer

Réunissez les éléments suivants avant de configurer iDRAC :

- *Guide d'utilisation de Dell Chassis Management Controller*
- CD *Dell PowerEdge Installation and Server Management*
- CD *Dell Systems Management Consoles*
- CD *Dell PowerEdge Service and Diagnostic Utilities*
- CD *Dell PowerEdge Documentation*

Interfaces de configuration d'iDRAC

Vous pouvez configurer iDRAC via l'utilitaire de configuration iDRAC, l'interface Web iDRAC, la CLI RACADM locale ou la CLI SM-CLP. La CLI RACADM locale est disponible une fois que vous avez installé le système d'exploitation et le logiciel de gestion de serveur Dell PowerEdge sur le serveur géré. Le tableau 2-1 décrit ces interfaces.

AVIS : L'utilisation de plusieurs interfaces de configuration simultanément peut provoquer des résultats inattendus.

Tableau 2-1. Interfaces de configuration

Interface	Description
Utilitaire de configuration iDRAC	L'utilitaire de configuration iDRAC, auquel il est possible d'accéder au démarrage, est particulièrement utile lors de l'installation d'un nouveau serveur PowerEdge. Utilisez-le pour configurer le réseau et les fonctionnalités de sécurité de base, ainsi que pour activer d'autres fonctionnalités.
Interface Web iDRAC	L'interface Web iDRAC est une application de gestion de type navigateur que vous pouvez utiliser pour gérer iDRAC de manière interactive et surveiller le serveur géré. Il s'agit de l'interface principale servant à l'exécution des tâches quotidiennes, comme par exemple la surveillance de l'intégrité du système, l'affichage du journal des événements système, la gestion des utilisateurs iDRAC locaux, et le lancement de l'interface Web CMC et des sessions de redirection de console.
Interface Web CMC	Outre la surveillance et la gestion du châssis, l'interface Web CMC peut être utilisée pour afficher la condition d'un serveur géré, configurer les paramètres réseau iDRAC et pour démarrer, arrêter ou réinitialiser le serveur géré.
Écran LCD du châssis	L'écran LCD du châssis contenant iDRAC peut être utilisé pour afficher la condition de niveau élevé des serveurs dans le châssis. Lors de la configuration initiale de CMC, l'Assistant de configuration vous permet d'activer la configuration DHCP de la mise en réseau d'iDRAC.
RACADM locale	L'interface de ligne de commande RACADM locale s'exécute sur le serveur géré. Elle est accessible depuis iKVM ou une session de redirection de console déclenchée à partir de l'interface Web iDRAC. RACADM est installé sur le serveur géré lorsque vous installez Dell OpenManage Server Administrator. Les commandes RACADM permettent d'accéder à quasiment toutes les fonctionnalités iDRAC. Vous pouvez inspecter les données du capteur, les enregistrements du journal des événements système, et la condition actuelle et les valeurs de configuration conservés dans iDRAC. Vous pouvez modifier les valeurs de configuration iDRAC, gérer les utilisateurs locaux, activer et désactiver les fonctionnalités et exécuter des fonctions d'alimentation, comme par exemple l'arrêt ou le redémarrage du serveur géré.
iVM-CLI	L'interface de ligne de commande du média virtuel iDRAC (iVM-CLI) permet au serveur géré d'accéder au média sur la station de gestion. Elle est particulièrement utile pour développer des scripts permettant d'installer des systèmes d'exploitation sur plusieurs serveurs gérés.
SM-CLP	SM-CLP est l'implémentation du protocole SM-CLP (Server Management-Command Line Protocol) du groupe de travail de gestion de serveur incorporé dans iDRAC. La ligne de commande SM-CLP est accessible en se connectant à iDRAC via Telnet ou SSH. Les commandes SM-CLP permettent d'implémenter un sous-ensemble, particulièrement utile, des commandes RACADM locales. Ces commandes sont utiles pour l'écriture de scripts car elles peuvent être exécutées à partir d'une ligne de commande de la station de gestion. La sortie des commandes peut être récupérée dans des formats bien définis, y compris le format XML, facilitant ainsi l'écriture de scripts et l'intégration avec les outils de génération de rapports et de gestion existants. Voir Équivalences RACADM et SM-CLP pour pouvoir comparer les commandes RACADM et SM-CLP.
IPMI	IPMI définit une méthode standard permettant aux sous-systèmes de gestion intégrés, comme par exemple iDRAC, de communiquer

	avec d'autres systèmes intégrés et applications de gestion. Vous pouvez utiliser l'interface Web iDRAC, les commandes SM-CLP ou RACADM pour configurer les filtres d'événements sur plateforme (PEF) et interruptions d'événements sur plateforme (PET) IPMI. Les filtres d'événements sur plateforme obligent iDRAC à effectuer des actions sélectionnables (par exemple, le redémarrage du serveur géré) lorsqu'une condition est détectée. Les interruptions d'événements sur plateforme ordonnent à iDRAC d'envoyer des alertes IPMI ou par e-mail lorsqu'il détecte des événements ou conditions spécifié(e)s. Vous pouvez également utiliser les outils IPMI standard tels que **ipmitool** et **ipmishell** avec iDRAC lorsque vous activez IPMI sur le LAN.

Tâches de configuration

Cette section est une présentation des tâches de configuration inhérentes à la station de gestion, à iDRAC et au serveur géré. Les tâches à effectuer incluent la configuration d'iDRAC afin de pouvoir l'utiliser à distance, la configuration des fonctionnalités iDRAC que vous souhaitez utiliser, l'installation du système d'exploitation sur le serveur géré et l'installation du logiciel de gestion sur votre station de gestion et sur le serveur géré.

Les tâches de configuration pouvant être utilisées pour effectuer chaque tâche sont répertoriées sous la tâche.

REMARQUE : Pour pouvoir effectuer les procédures de configuration dans ce guide, les modules d'E/S et CMC doivent être installés dans le châssis et configurés, et le serveur PowerEdge doit être physiquement installé dans le châssis.

Configurer la station de gestion

Configurez une station de gestion en installant le logiciel Dell OpenManage, un navigateur Web et d'autres utilitaires de logiciel.

- Voir Configuration de la station de gestion

Configurer la mise en réseau iDRAC

Activez le réseau iDRAC et configurez les adresses IP, de masque réseau, de passerelle et DNS.

REMARQUE : La modification des paramètres réseau iDRAC met fin à toutes les connexions réseau actuelles sur iDRAC.

REMARQUE : L'option permettant de configurer le serveur via l'écran LCD est disponible *uniquement* lors de la configuration CMC initiale. Une fois le châssis déployé, l'écran LCD ne peut pas être utilisé pour reconfigurer iDRAC.

REMARQUE : L'écran LCD peut être utilisé pour activer DHCP pour configurer le réseau iDRAC. Si vous souhaitez attribuer des adresses statiques, vous devez utiliser l'utilitaire de configuration iDRAC ou l'interface Web CMC.

- Écran LCD du châssis : voir le *Guide d'utilisation de Dell Chassis Management Controller*.
- Utilitaire de configuration iDRAC : voir LAN
- Interface Web CMC : voir Configuration de la mise en réseau via l'interface Web CMC
- RACADM : voir cfgLanNetworking

Configurer les utilisateurs iDRAC

Configurez les utilisateurs iDRAC locaux ainsi que leurs droits. iDRAC intègre un tableau de seize utilisateurs locaux dans le micrologiciel. Vous pouvez définir les noms d'utilisateur, mots de passe et rôles pour ces utilisateurs.

- Utilitaire de configuration iDRAC (configure l'utilisateur d'administration uniquement) : voir Configuration utilisateur LAN
- Interface Web iDRAC : voir Ajout et configuration des utilisateurs iDRAC
- RACADM : voir Ajout d'un utilisateur iDRAC

Configurer Active Directory

Outre les utilisateurs iDRAC locaux, vous pouvez utiliser Microsoft® Active Directory® pour authentifier les ouvertures de session utilisateur iDRAC.

- Voir Utilisation d'iDRAC avec Microsoft Active Directory

Configurer le filtrage IP et le blocage IP

Outre l'authentification utilisateur, vous pouvez empêcher l'accès non autorisé en rejetant les tentatives de connexion des adresses IP hors d'une plage définie et en bloquant temporairement les connexions des adresses IP auxquelles l'authentification a échoué à plusieurs reprises dans un laps de temps configurable.

- Interface Web iDRAC : voir Configuration du filtrage IP et du blocage IP
- RACADM : voir Configuration du filtrage IP (IpRange), Configuration du blocage IP

Configurer les événements sur plateforme

Les événements sur plateforme se produisent lorsqu'iDRAC détecte un avertissement ou une condition critique provenant de l'un des capteurs du serveur géré.

Configurez les filtres d'événements sur plateforme (PEF) pour choisir les événements que vous souhaitez détecter, comme par exemple le redémarrage du serveur géré, lorsqu'un événement est détecté.

- Interface Web iDRAC : voir Configuration des filtres d'événements sur plateforme (PEF)
- RACADM : voir Configuration de PEF

Configurez les interruptions d'événements sur plateforme (PET) pour envoyer des notifications d'alerte à une adresse IP, telle qu'une station de gestion avec le logiciel IPMI ou pour envoyer un e-mail à une adresse e-mail spécifiée.

- Interface Web iDRAC : voir Configuration des interruptions d'événement sur plateforme (PET)
- RACADM : Configuration de PET

Configurer les communications série sur le LAN

Les communications série sur le LAN (SOL) sont une fonctionnalité IPMI vous permettant de rediriger l'E/S du port série du serveur géré sur le réseau. SOL active la fonctionnalité de redirection de console iDRAC.

- Interface Web iDRAC : voir Configuration des communications série sur le LAN
- Voir aussi Utilisation de la redirection de console d'interface utilisateur graphique

Configurer les services iDRAC

Activez ou désactivez les services réseau iDRAC, comme par exemple Telnet, SSH et l'interface Web Server, et reconfigurez les ports et autres paramètres de services.

- Interface Web iDRAC : voir Configuration des services iDRAC
- RACADM : voir Configuration de services Telnet et SSH iDRAC via RACADM local

Configurer le protocole Secure Sockets Layer (SSL)

Configurez le protocole SSL pour Web Server iDRAC.

- Interface Web iDRAC : voir Protocole Secure Sockets Layer (SSL)
- RACADM : voir cfgRacSecurity, sslcsrgen, sslcertupload, sslcertdownload, sslcertview

Configurer le média virtuel

Configurez la fonctionnalité de média virtuel afin de pouvoir installer le système d'exploitation sur le serveur PowerEdge. Le média virtuel permet au serveur géré d'accéder aux périphériques de média présents sur la station de gestion ou aux images de CD/DVD ISO sur un partage réseau comme s'il s'agissait de périphériques du serveur géré.

- Interface Web iDRAC : voir Configuration et utilisation du média virtuel
- Utilitaire de configuration iDRAC : voir Média virtuel

Installer le logiciel Managed Server

Installez le système d'exploitation Microsoft Windows ou Linux sur le serveur PowerEdge à l'aide du média virtuel, puis installez le logiciel Dell OpenManage sur le serveur PowerEdge géré et configurez la fonctionnalité Écran de la dernière panne.

- Redirection de console : voir Installation du logiciel sur le serveur géré
- iVM-CLI : voir Utilisation de l'utilitaire d'interface de ligne de commande de média virtuel

Configurer le serveur géré pour la fonctionnalité Écran de la dernière panne

Configurez le serveur géré de manière à ce qu'iDRAC puisse capturer l'image de l'écran après un plantage ou un blocage du système d'exploitation.

- Serveur géré : voir Configuration du serveur géré pour la saisie de l'écran de la dernière panne, Désactivation de l'option de redémarrage automatique

de Windows

Configuration de la mise en réseau via l'interface Web CMC

REMARQUE : Vous devez disposer du privilège Administrateur et configuration du châssis pour pouvoir configurer les paramètres réseau iDRAC à partir de CMC.

REMARQUE : L'utilisateur CMC par défaut est **root** et le mot de passe par défaut est **calvin**.

REMARQUE : Vous pouvez accéder à l'adresse IP CMC dans l'interface Web iDRAC en cliquant sur **Système→ Accès à distance→ CMC**. Vous pouvez également lancer l'interface Web CMC à partir de cette page.

1. Utilisez votre navigateur Web pour vous connecter à l'interface utilisateur Web CMC via une adresse URL sous la forme https://<*adresse IP CMC*> ou https://<*nom DNS CMC*>.
2. Entrez le nom d'utilisateur et le mot de passe CMC, puis cliquez sur **OK**.
3. Cliquez sur le signe plus (+) situé en regard de **Châssis** dans la colonne de gauche, puis cliquez sur **Serveurs**.
4. Cliquez sur **Configuration→ Déployer.**
5. Activez le LAN du serveur en cochant la case à cocher située en regard du serveur sous l'en-tête **Activer le LAN**.
6. Activez ou désactivez IPMI sur le LAN en cochant ou décochant la case à cocher située en regard du serveur sous l'en-tête **Activer IPMI sur le LAN**.
7. Activez ou désactivez DHCP pour le serveur en cochant ou décochant la case à cocher située en regard du serveur sous l'en-tête **Protocole DHCP activé**.
8. Si DHCP est désactivé, entrez l'adresse IP statique, le masque réseau et la passerelle par défaut du serveur.
9. Cliquez sur **Appliquer** au bas de la page.

Mise à jour du micrologiciel iDRAC

La mise à jour du micrologiciel iDRAC installe une nouvelle image de micrologiciel dans la mémoire Flash iDRAC. Vous pouvez mettre à jour le micrologiciel à l'aide de l'une des méthodes suivantes :

- Commande **load** SM-CLP
- Interface Web iDRAC
- Progiciel de mise à jour Dell (pour Linux ou Microsoft Windows)
- Utilitaire de mise à jour de micrologiciel iDRAC DOS
- Interface Web CMC (uniquement si le micrologiciel iDRAC est corrompu)

Téléchargement du micrologiciel ou du progiciel de mise à jour

Téléchargez le micrologiciel à l'adresse **support.dell.com**. L'image de micrologiciel est disponible dans plusieurs formats différents pour pouvoir prendre en charge les diverses méthodes de mise à jour disponibles.

Pour mettre à jour le micrologiciel iDRAC via l'interface Web iDRAC ou SM-CLP, ou pour récupérer iDRAC via l'interface Web CMC, téléchargez l'image binaire qui se présente sous la forme d'une archive à extraction automatique.

Pour mettre à jour le micrologiciel iDRAC à partir du serveur géré, téléchargez le progiciel de mise à jour Dell (DUP) spécifique au système d'exploitation qui s'exécute sur le serveur dont l'iDRAC est mis à jour.

Pour mettre à jour le micrologiciel iDRAC à l'aide de l'utilitaire de mise à jour de micrologiciel iDRAC DOS, téléchargez l'utilitaire de mise à jour et l'image binaire, qui se présentent sous la forme d'archives à extraction automatique.

Exécuter la mise à jour de micrologiciel

REMARQUE : Lorsque la mise à jour de micrologiciel iDRAC commence, toutes les sessions iDRAC existantes sont déconnectées et les nouvelles sessions ne sont pas autorisées tant que le processus de mise à jour n'est pas terminé.

REMARQUE : Les ventilateurs du châssis s'exécutent à 100 % lors de la mise à jour de micrologiciel iDRAC. Lorsque la mise à jour est terminée, la régulation de la vitesse normale du ventilateur reprend. Il s'agit d'un comportement normal visant à protéger le serveur contre toute surchauffe durant le laps de temps au cours duquel il ne peut pas envoyer d'informations de capteur à CMC.

Pour utiliser un progiciel de mise à jour Dell pour Linux ou Microsoft Windows, exécutez le progiciel de mise à jour Dell spécifique au système d'exploitation qui

s'exécute sur le serveur géré.

Lors de l'utilisation de la commande **load** SM-CLP, placez l'image binaire du micrologiciel dans un répertoire à partir duquel un serveur TFTP (Protocole simplifié de transfert de fichiers) pourra l'adresser à iDRAC. Voir Mise à jour du micrologiciel iDRAC via SM-CLP.

Lorsque vous utilisez l'interface Web iDRAC ou l'interface Web CMC, placez l'image binaire du micrologiciel sur un disque accessible à la station de gestion à partir de laquelle vous exécutez l'interface Web. Voir Mise à jour du micrologiciel iDRAC.

REMARQUE : L'interface Web iDRAC vous permet également de rétablir les paramètres d'usine de la configuration iDRAC.

Vous pouvez utiliser l'interface Web CMC pour mettre à jour le micrologiciel *uniquement* lorsque CMC détecte que le micrologiciel iDRAC est corrompu, ce qui peut se produire lorsque la progression de la mise à jour de micrologiciel iDRAC est interrompue avant qu'elle ne se termine. Voir Récupération du micrologiciel iDRAC à l'aide de CMC.

Utilisation de l'utilitaire de mise à jour DOS

Pour mettre à jour le micrologiciel iDRAC à l'aide de l'utilitaire de mise à jour DOS, démarrez le serveur géré sur DOS et exécutez la commande **idrac16d**. La syntaxe de la commande est la suivante :

```
idrac16d [-f] [-i=<nom de fichier>] [-l=<fichier journal>]
```

Lorsqu'elle est exécutée sans option, la commande **idrac16d** met à jour le micrologiciel iDRAC à l'aide du fichier image de micrologiciel **firmimg.imc** dans le répertoire actuel.

Les options sont les suivantes :

`-f` : force la mise à jour. L'option `-f` peut être utilisée pour *rétrograder* le micrologiciel à une image antérieure.

`-i=<nom de fichier>` : spécifie l'image du nom de fichier qui contient l'image de micrologiciel. Cette option est requise si le nom de fichier par défaut **firmimg.imc** du micrologiciel a été modifié.

-l=<*fichier journal*> : consigne le résultat de l'activité de mise à jour. Cette option est utilisée pour le débogage.

AVIS : Si vous entrez des arguments incorrects dans la commande **idrac16d,** ou spécifiez l'option `-h`, il se peut qu'une option supplémentaire, `-nopresconfig`, apparaisse dans le résultat d'utilisation. Cette option est utilisée pour mettre à jour le micrologiciel sans conserver les informations sur la configuration. Vous **ne devez pas** utiliser cette option car elle *supprime* toutes vos informations de configuration iDRAC existantes, notamment les adresses IP, utilisateurs et mots de passe.

Vérification de la signature numérique

Une signature numérique sert à authentifier l'identité du signataire d'un fichier et à certifier que le contenu d'origine du fichier n'a pas été modifié depuis qu'il a été signé.

Si vous ne l'avez pas encore installé sur votre système, vous devez installer le dispositif de protection GPG (Gnu Privacy Guard) pour vérifier une signature numérique. Pour utiliser la procédure de vérification standard, effectuez les étapes suivantes :

1. Téléchargez la clé GnuPG publique Dell Linux, si vous ne l'avez pas déjà, en accédant au site **lists.us.dell.com** et en cliquant sur le lien **Dell Public GPG key**. Enregistrez le fichier sur votre système local. Le nom par défaut est **linux-security- publickey.txt**.

2. Importez la clé publique dans votre base de données sécurisée gpg en exécutant la commande suivante :

   ```
   gpg --import <Nom de fichier de la clé publique>
   ```

   REMARQUE : Vous devez disposer de votre clé privée pour terminer le processus.

3. Pour éviter un avertissement de clé non approuvée, modifiez le niveau de confiance de la clé GPG publique Dell.

   a. Tapez la commande suivante :

      ```
      gpg --edit-key 23B66A9D
      ```

   b. Dans l'éditeur de clé GPG, tapez `fpr`. Le message suivant apparaît :

      ```
      pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group) <linux-security@dell.com>
      Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
      ```

      Si l'empreinte de votre clé importée est identique à l'empreinte ci-dessus, cela signifie que votre copie de la clé est correcte.

   c. Toujours dans l'éditeur de clé GPG, tapez `trust`. Le menu suivant apparaît :

      ```
      Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
      different sources, etc.)

        1 = I don't know or won't say
        2 = I do NOT trust
        3 = I trust marginally
        4 = I trust fully
        5 = I trust ultimately
        m = back to the main menu
      ```

```
Your decision?

(Veuillez préciser à quel point vous faites confiance à cet utilisateur pour vérifier correctement les clés des autres utilisateurs
(en examinant les passeports, en vérifiant les empreintes à partir de différentes sources, etc.)

  1 = Je ne sais pas ou préfère ne pas me prononcer
  2 = Je NE fais PAS confiance
  3 = Je fais partiellement confiance
  4 = Je fais entièrement confiance
  5 = Je fais définitivement confiance
  m = retour au menu principal

Votre décision ?)
```

d. Tapez 5 <Entrée>. L'invite suivante apparaît :

```
Do you really want to set this key to ultimate trust? (y/N)

(Souhaitez-vous définir cette clé sur le niveau de confiance définitive ? (y/N))
```

e. Tapez y <Entrée> pour confirmer votre choix.

f. Tapez quit <Entrée> pour quitter l'éditeur de clé GPG.

Vous devez importer et valider la clé publique à une seule reprise.

4. Procurez-vous le progiciel dont vous avez besoin, par exemple le progiciel de mise à jour Dell Linux ou l'archive à extraction automatique) et le fichier de signature qui lui est associé sur le site Web de support de Dell à l'adresse **support.dell.com / support / downloads**.

REMARQUE : Chaque progiciel de mise à jour Linux dispose d'un fichier de signature distinct, qui s'affiche sur la même page Web que le progiciel de mise à jour. Il vous faut le progiciel de mise à jour et le fichier de signature qui lui est associé pour la vérification. Par défaut, le fichier de signature porte le même nom que le fichier DUP avec une extension **.sign**. Ainsi, si un fichier DUP Linux s'intitule **PE1850-BIOS-LX-A02.BIN**, son fichier de signature s'intitule **PE1850-BIOS-LX-A02.BIN.sign**. L'image de micrologiciel iDRAC possède également un fichier **.sign** associé, inclus dans l'archive à extraction automatique avec l'image de micrologiciel. Pour télécharger les fichiers, cliquez-droite sur le lien de téléchargement et utilisez l'option de fichier **Enregistrer la cible sous...**.

5. Vérifiez le progiciel de mise à jour :

```
gpg --verify <nom de fichier de signature du progiciel de mise à jour Linux> <nom de fichier du progiciel de mise à jour Linux>
```

L'exemple suivant illustre les étapes à suivre pour vérifier un progiciel de mise à jour du BIOS 1425SC :

1. Téléchargez les deux fichiers suivants à l'adresse **support.dell.com** :
   - PESC1425-BIOS-LX-A01.bin.sign
   - PESC1425-BIOS-LX-A01.bin

2. Importez la clé publique en exécutant la ligne de commande suivante :

```
gpg --import <linux-security-publickey.txt>
```

Le message de sortie suivant apparaît :

```
gpg: key 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
```

3. Définissez le niveau de confiance GPG de la clé publique Dell si vous ne l'avez pas encore fait.

a. Tapez la commande suivante :

```
gpg --edit-key 23B66A9D
```

b. À l'invite de commande, tapez les commandes suivantes :

```
fpr
trust
```

c. Tapez 5 <Entrée> pour choisir `I trust ultimately (Je fais définitivement confiance)` dans le menu.

d. Tapez y <Entrée> pour confirmer votre choix.

e. Tapez quit <Entrée> pour quitter l'éditeur de clé GPG.

Cette opération termine la validation de la clé publique Dell.

4. Vérifiez la signature numérique du progiciel du BIOS PESC1425 en exécutant la commande suivante :

```
gpg --verify PESC1425-BIOS-LX-A01.bin.sign PESC1425-BIOS-LX-A01.bin
```

Le message de sortie suivant apparaît :

```
gpg: Signature made Thu 14 Apr 2005 04:25:37 AM IST using DSA key ID 23B66A9D
gpg: Good signature from "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>"
```

REMARQUE : Si vous n'avez pas validé la clé comme illustré à l'étape 3, vous recevrez des messages supplémentaires :

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
```

Retour à la page du sommaire

Retour à la page du sommaire

Configuration de la station de gestion

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Une station de gestion est un ordinateur servant à surveiller et à gérer les serveurs PowerEdge ainsi que les autres modules du châssis. Cette section décrit l'installation logicielle et les tâches de configuration permettant de configurer une station de gestion afin qu'elle puisse fonctionner avec iDRAC. Avant de commencer à configurer iDRAC, suivez les procédures de cette section afin de vous assurer que vous avez installé et configuré les outils nécessaires.

Étapes de configuration de la station de gestion

Pour configurer votre station de gestion, effectuez les étapes suivantes :

1. Configurez le réseau de la station de gestion.
2. Installez et configurez un navigateur Web pris en charge.
3. Installez un environnement d'exécution Java (JRE) (facultatif pour Windows).
4. Installez les clients Telnet ou SSH, si nécessaire.
5. Installez un serveur TFTP, si nécessaire.
6. Installez Dell OpenManage IT Assistant (facultatif).

Impératifs de réseau de la station de gestion

Pour accéder à iDRAC, la station de gestion doit se trouver sur le même réseau que le port de connexion RJ45 CMC appelé « GB1 ». Il est possible d'isoler le réseau CMC du réseau sur lequel se trouve le serveur géré, de sorte que votre station de gestion puisse disposer d'un accès LAN à iDRAC, mais non au serveur géré.

Grâce à la fonctionnalité de redirection de console iDRAC (voir Utilisation de la redirection de console d'interface utilisateur graphique), vous pouvez accéder à la console du serveur géré même si vous ne disposez pas d'un accès réseau aux ports du serveur. Vous pouvez également exécuter plusieurs fonctions de gestion sur le serveur géré, comme par exemple le redémarrage de l'ordinateur, à l'aide des services iDRAC. Pour accéder aux services réseau et d'application hébergés sur le serveur géré, il vous faudra peut-être cependant un NIC supplémentaire sur l'ordinateur de gestion.

Configuration d'un navigateur Web pris en charge

Les sections suivantes fournissent des instructions en vue de la configuration des navigateurs Web pris en charge afin de les utiliser avec l'interface Web iDRAC. Vous trouverez une liste des navigateurs Web pris en charge dans la section Navigateurs Web pris en charge.

REMARQUE : L'interface Web iDRAC 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 à iDRAC.

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

Si vous vous connectez à l'interface Web iDRAC 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 le navigateur Web Internet Explorer pour accéder à un serveur proxy, effectuez les étapes suivantes :

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.

Ajout d'iDRAC à la liste des domaines de confiance

Lorsque vous accédez à l'interface Web iDRAC via le navigateur, vous devrez peut-être ajouter l'adresse IP iDRAC 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 établir une connexion à l'interface Web iDRAC.

Affichage des versions localisées de l'interface Web

L'interface Web iDRAC est prise en charge par les langues suivantes du système d'exploitation :

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

Internet Explorer 6.0 (Windows)

Pour afficher une version localisée de l'interface Web iDRAC dans Internet Explorer, effectuez les étapes suivantes :

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. Dans la fenêtre **Langues**, cliquez sur **OK**.
7. Cliquez sur **OK**.

Firefox 1.5 (Linux)

Pour afficher une version localisée de l'interface Web iDRAC dans Firefox, effectuez les étapes suivantes :

1. Cliquez sur **Édition**→ **Préférences**, puis cliquez sur l'onglet **Avancé**.
2. Dans la section **Langue**, cliquez sur **Choisir**.
3. Cliquez sur **Sélectionner une langue à ajouter...**.
4. Sélectionnez une langue prise en charge et cliquez sur **Ajouter**.
5. Sélectionnez la langue de votre choix et cliquez sur **Monter** pour la déplacer en haut de la liste.
6. Dans le menu Langues, cliquez sur **OK**.
7. Cliquez sur **OK**.

Configuration des paramètres régionaux sous Linux

Le visualiseur de redirection de console requiert un jeu de caractères UTF-8 pour pouvoir s'afficher correctement. Si votre affichage est tronqué, vérifiez vos paramètres régionaux et réinitialisez le jeu de caractères si besoin.

Les étapes suivantes illustrent la façon de configurer le jeu de caractères sur un client Red Hat® Enterprise Linux® doté d'une interface utilisateur en chinois simplifié :

1. Ouvrez un terminal de commande.
2. Tapez locale et appuyez sur <Entrée>. Un résultat semblable au suivant est obtenu :

```
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. Modifiez le fichier **/etc/sysconfig/i18n** à l'aide d'un éditeur de texte.
5. Dans le fichier, appliquez les changements suivants :

   Entrée actuelle :

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

   Entrée changée :

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

6. Fermez la session et connectez-vous au système d'exploitation.

Lorsque vous passez d'une langue à l'autre, assurez-vous que ce correctif est toujours valide. Sinon, répétez cette procédure.

Désactivation de la fonctionnalité de liste blanche dans Firefox

Firefox intègre une fonctionnalité de sécurité de « liste blanche » qui requiert une autorisation utilisateur pour installer des plug-ins pour chaque site distinct hébergeant un plug-in. Si elle est activée, la fonctionnalité de liste blanche vous oblige à installer un visualiseur de redirection de console pour chaque iDRAC visité, même si les versions de visualiseur sont identiques.

Pour désactiver la fonctionnalité de liste blanche et éviter toute installation de plug-in inutile, effectuez les étapes suivantes :

1. Ouvrez une fenêtre de navigateur Web Firefox.
2. Dans le champ d'adresse, tapez `about:config` et appuyez sur <Entrée> :
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 **Condition** devient **défini par l'utilisateur** et celle de **Valeur** devient **faux**.
4. Dans la colonne **Préférences Nom**, recherchez **xpinstall.enabled**.

   Assurez-vous que **Valeur** est défini sur **true**. Si ce n'est pas le cas, double-cliquez sur **xpinstall.enabled** pour définir **Valeur** sur **true**.

Installation d'un environnement d'exécution Java (JRE)

REMARQUE : Si vous utilisez le navigateur Internet Explorer, un contrôle ActiveX est fourni pour le visualiseur de console. Vous pouvez également utiliser le visualiseur de console Java avec Internet Explorer si vous installez un JRE et configurer le visualiseur de console dans l'interface Web iDRAC

avant de lancer le visualiseur. Voir Configuration de la redirection de console dans l'interface Web iDRAC pour plus d'informations.

Vous pouvez choisir d'utiliser le visualiseur Java à la place avant de lancer le visualiseur.

Si vous utilisez le navigateur Firefox, vous devez installer un JRE (ou un kit de développement Java [JDK]) pour pouvoir utiliser la fonctionnalité de redirection de console. Le visualiseur de console est une application Java téléchargée sur la station de gestion à partir de l'interface Web iDRAC, puis lancée via Java Web Start sur la station de gestion.

Allez sur le site **java.sun.com** pour installer un JRE ou JDK. La version 1.6 (Java 6.0) ou ultérieure est recommandée.

Installation de clients Telnet ou SSH

Par défaut, le service Telnet iDRAC est désactivé et le service SSH est activé. Étant donné que Telnet est un protocole non sécurisé, vous devez uniquement l'utiliser si vous ne pouvez pas installer un client SSH ou si votre connexion réseau est sécurisée.

REMARQUE : Une seule connexion Telnet ou SSH peut être active à la fois sur iDRAC. Lorsqu'une connexion est active, toutes les autres tentatives de connexion sont refusées.

Telnet avec iDRAC

Telnet est inclus dans les systèmes d'exploitation Microsoft® Windows® et Linux, et peut être exécuté à partir d'un environnement de commande. Vous pouvez également opter pour l'installation d'un client Telnet commercial ou disponible librement doté de fonctionnalités plus conviviales que celles de la version standard intégrée à votre système d'exploitation.

Si votre station de gestion exécute Windows XP ou Windows 2003, vous pouvez rencontrer un problème de caractères dans une session Telnet iDRAC. 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**. Voir l'article 824810 de la base de connaissances Microsoft pour plus d'informations.

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><]>.
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 un environnement et tapez :

   ```
   stty erase ^h
   ```
2. À l'invite, tapez :

   ```
   telnet
   ```

SSH avec iDRAC

Secure Shell (SSH) est une connexion de ligne de commande ayant les mêmes fonctions qu'une session Telnet, mais intégrant la négociation de session et le cryptage pour améliorer la sécurité. iDRAC prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé par défaut sur iDRAC.

Vous pouvez utiliser PuTTY (Windows) ou OpenSSH (Linux) sur une station de gestion pour vous connecter à l'iDRAC du serveur géré. Lorsqu'une erreur se

produit pendant la procédure d'ouverture de session, le client **ssh** publie un message d'erreur. Le texte du message dépend du client et n'est pas contrôlé par iDRAC.

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).

Une seule session Telnet ou SSH est prise en charge à la fois. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout` comme indiqué dans la section Définitions des groupes et des objets de la base de données des propriétés iDRAC.

L'implémentation SSH iDRAC prend en charge plusieurs projets de cryptographie, comme illustré dans le tableau 3-1.

REMARQUE : SSHv1 n'est pas pris en charge.

Tableau 3-1. Schémas de cryptographie

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

Installation d'un serveur TFTP

REMARQUE : Si vous utilisez uniquement l'interface Web iDRAC pour transférer des certificats SSL et téléverser un nouveau micrologiciel iDRAC, aucun serveur TFTP n'est requis.

Le protocole simplifié de transfert de fichiers (TFTP) est une forme simplifiée du protocole FTP. Il est utilisé avec les interfaces de ligne de commande SM-CLP et RACADM pour transférer des fichiers à destination et en provenance d'iDRAC.

Vous devez uniquement copier des fichiers à destination ou en provenance d'iDRAC lorsque vous mettez à jour le micrologiciel iDRAC ou installez des certificats sur iDRAC. Si vous choisissez d'utiliser la commande SM-CLP ou RACADM lorsque vous effectuez ces tâches, un serveur TFTP doit s'exécuter sur un ordinateur auquel iDRAC peut avoir accès par numéro IP ou nom DNS.

Vous pouvez utiliser la commande **netstat -a** sur les systèmes d'exploitation Windows ou Linux afin de déterminer si un serveur TFTP écoute déjà. Le port 69 est le port du serveur TFTP par défaut. Si aucun serveur ne s'exécute, les options suivantes s'offrent à vous :

- Recherchez un autre ordinateur sur le réseau exécutant un service TFTP
- Si vous utilisez Linux, installez un serveur TFTP à partir de votre distribution
- Si vous utilisez Windows, installez un serveur TFTP commercial ou gratuit

Installation de Dell OpenManage IT Assistant

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

- CD *Dell Systems Management Consoles* : contient tous les derniers produits de la console Dell Systems Management, y compris Dell OpenManage IT Assistant.
- CD *Dell PowerEdge Service and Diagnostic Utilities* : fournit les outils dont vous avez besoin pour configurer votre système et vous apporte les micrologiciels, diagnostics et pilotes optimisés par Dell pour votre système.
- CD *Dell PowerEdge Documentation* : vous permet d'être informé sur les systèmes, les produits Systems Management Software, les périphériques et les contrôleurs RAID.
- Site Web de support de Dell et fichiers « Lisez-moi » : consultez les fichiers « Lisez-moi » et le site Web de support de Dell à l'adresse **support.dell.com** pour obtenir les dernières informations sur vos produits Dell.

Utilisez le CD *Dell System Management Consoles* pour installer le logiciel de console de gestion, y compris Dell OpenManage IT Assistant, sur la station de gestion. Pour obtenir des instructions sur l'installation de ce logiciel, consultez votre *Guide d'installation rapide*.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration du serveur géré

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Cette section décrit les tâches permettant de configurer le serveur géré afin d'optimiser vos fonctions de gestion à distance. Ces tâches incluent l'installation du logiciel Dell Open Manage Server Administrator et la configuration du serveur géré pour capturer l'écran de la dernière panne.

Installation du logiciel sur le serveur géré

Le logiciel de gestion Dell inclut les fonctionnalités suivantes :

- CLI RACADM locale : vous permet de configurer et d'administrer iDRAC à partir du système géré. Il s'agit d'un outil puissant permettant d'écrire des scripts de configuration et de gestion des tâches.
- Server Administrator est requis pour utiliser la fonctionnalité Écran de la dernière panne iDRAC.
- Server Administrator : interface Web qui vous permet d'administrer le système distant depuis un hôte distant sur le réseau.
- Server Administrator Instrumentation Service : permet d'accéder aux informations détaillées sur les anomalies et les performances recueillies par les agents Systems Management standard du secteur et autorise l'administration à distance des systèmes surveillés, y compris l'arrêt, le démarrage et la sécurité.
- Service Server Administration Storage Management : fournit des informations sur Storage Management dans un affichage graphique intégré.
- Journaux Server Administrator : affichent des journaux de commandes émises sur ou par le système, d'événements de matériel surveillés, d'événements POST et d'alertes du système. Vous pouvez afficher les journaux sur la page d'accueil, les imprimer ou les enregistrer sous forme de rapports et les envoyer par e-mail à un contact de service désigné.

Utilisez le CD *Dell PowerEdge Installation and Server Management* pour installer Server Administrator. Pour obtenir des instructions sur l'installation de ce logiciel, consultez votre *Guide d'installation rapide*.

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

iDRAC peut capturer l'écran de la dernière panne afin que vous puissiez l'afficher dans l'interface Web afin de vous permettre de définir la cause du plantage du système géré et d'y remédier. Suivez les étapes suivantes pour activer la fonctionnalité Écran de la dernière panne.

1. Installez le logiciel Managed Server. Pour des informations supplémentaires sur l'installation du logiciel Managed Server Software, voir le *Guide d'utilisation de Server Administrator*.

2. Si vous exécutez un système d'exploitation Microsoft® Windows®, assurez-vous que la fonctionnalité Redémarrage automatique est désélectionnée dans les **paramètres de démarrage et de récupération de Windows**. Voir Désactivation de l'option de redémarrage automatique de Windows.

3. Activez l'écran de la dernière panne (désactivé par défaut) dans l'interface Web iDRAC.

   Pour activer l'écran de la dernière panne dans l'interface Web iDRAC, cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services**, puis cochez la case **Activer** sous l'en-tête Paramètres d'agent de récupération automatique du système.

   Pour activer l'écran de la dernière panne via RACADM local, ouvrez une invite de commande sur le système géré et tapez la commande suivante :

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

4. Dans l'interface Web de Server Administrator, activez l'**horloge de récupération automatique** et définissez l'action **de récupération automatique** sur **Réintialiser**, **Mettre hors tension** ou **Cycle d'alimentation**.

   Pour plus d'informations sur la configuration de l'**horloge de récupération automatique**, voir 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. La valeur par défaut est 480 secondes.

   L'écran de la dernière panne n'est pas disponible lorsque l'**action de récupération automatique** est définie sur **Arrêt** ou **Cycle d'alimentation** si le système géré est hors tension.

Désactivation de l'option de redémarrage automatique de Windows

Pour s'assurer qu'iDRAC peut capturer l'écran de la dernière panne, désactivez l'option **Redémarrage automatique** sur les serveurs gérés exécutant Microsoft Windows Server® ou Windows Vista®.

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.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration d'iDRAC via l'interface Web

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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

La plupart des tâches de configuration d'interface Web peuvent également être effectuées avec des commandes RACADM locales ou avec des commandes SM-CLP.

Les commandes RACADM locales sont exécutées à partir du serveur géré. Pour plus d'informations sur les commandes RACADM locales, voir Utilisation de l'interface de ligne de commande RACADM locale.

Les commandes SM-CLP sont exécutées dans un environnement accessible à distance via une connexion Telnet ou SSH. Pour plus d'informations sur SM-CLP, voir Utilisation de l'interface de ligne de commande SM-CLP iDRAC.

Accès à l'interface Web

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

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

   Voir Navigateurs Web pris en charge pour plus d'informations.

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

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

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

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

   La fenêtre **Ouverture de session** iDRAC apparaît.

Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur iDRAC ou utilisateur Microsoft® Active Directory®. Par défaut, le nom d'utilisateur est **root** et le mot de passe est **calvin**.

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

Pour ouvrir une session, effectuez les étapes suivantes.

1. Dans le champ **Nom d'utilisateur**, tapez :
   - Votre nom d'utilisateur iDRAC.

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

     Les noms Active Directory peuvent être entrés sous la forme *<domaine>\<nom d'utilisateur>*, *<domaine>/<nom d'utilisateur>* ou *<utilisateur>@<domaine>*. Ils ne sont pas sensibles à la casse. Les exemples sont `dell.com\jean_dupont` ou `JEAN_DUPONT@DELL.COM`.
2. Dans le champ **Mot de passe**, tapez votre mot de passe utilisateur iDRAC ou Active Directory. Les mots de passe sont sensibles à la casse.
3. Cliquez sur **OK** ou appuyez sur <Entrée>.

Fermeture de session

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

2. Fermez la fenêtre du navigateur 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 peut rester ouverte jusqu'à ce qu'elle expire. Nous vous conseillons vivement de cliquer sur le bouton Fermer la session pour terminer la session ; sinon la session peut rester active jusqu'à ce que son délai d'expiration soit atteint.

REMARQUE : La fermeture de l'interface Web iDRAC 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 iDRAC

Cette section suppose qu'iDRAC a déjà été configuré et est accessible sur le réseau. Voir Configurer la mise en réseau iDRAC pour obtenir de l'aide sur la configuration réseau iDRAC initiale.

Configuration des paramètres réseau et LAN IPMI

REMARQUE : Vous devez disposer du privilège de **configuration iDRAC** 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 (iDRAC, par exemple) doit fournir ce jeton pendant la négociation DHCP. iDRAC 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.

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**.

2. Cliquez sur l'onglet **Réseau/Sécurité** pour ouvrir la page **Configuration réseau**.

   Le tableau 5-1 et le tableau 5-2 décrivent les **paramètres réseau** et les **paramètres LAN IPMI** sur la page **Réseau**.

3. Après avoir entré les paramètres requis, cliquez sur **Appliquer**.

4. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-3.

Tableau 5-1. Paramètres réseau

Paramètre	Description
Activer le NIC	Lorsqu'il est coché, ce paramètre indique que le NIC est activé et active les commandes restantes de ce groupe. Lorsqu'un NIC est désactivé, toutes les communications avec iDRAC via le réseau sont bloquées. La valeur par défaut est **désactivé**.
Adresse de contrôle de l'accès aux médias (MAC)	Affiche l'adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nœud d'un réseau. L'adresse MAC ne peut pas être modifiée.
Utiliser DHCP (pour l'adresse IP du NIC)	Demande à iDRAC d'obtenir une adresse IP pour le NIC sur le serveur de protocole de configuration dynamique d'hôte (DHCP). Désactive également les commandes **Adresse IP statique**, **Masque de sous-réseau statique** et **Passerelle statique**. La valeur par défaut est **désactivé**.
Adresse IP statique	Vous permet de saisir ou de modifier une adresse IP statique pour le NIC d'iDRAC. Pour modifier ce paramètre, décochez la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Masque de sous-réseau statique	Vous permet de saisir ou de modifier un masque de sous-réseau pour le NIC d'iDRAC. Pour modifier ce paramètre, commencez par décocher la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Passerelle statique	Vous permet de saisir ou de modifier une passerelle statique pour le NIC d'iDRAC. Pour modifier ce paramètre, commencez par décocher la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Utiliser DHCP pour obtenir des adresses de serveur DNS	Activez DHCP pour obtenir les adresses de serveur DNS en cochant la case **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Si vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS statique préféré** et **Autre serveur DNS statique**. La valeur par défaut est **désactivé**. **REMARQUE :** Lorsque la case **Utiliser DHCP pour obtenir des adresses de serveur DNS** est cochée, les adresses IP ne peuvent pas être entrées dans les champs **Serveur DNS statique préféré** et **Autre serveur DNS statique**.
Serveur DNS statique préféré	Permet à l'utilisateur de saisir ou de modifier une adresse IP statique pour le serveur DNS préféré. Pour modifier ce paramètre, commencez par décocher la case **Utiliser DHCP pour obtenir des adresses de serveur DNS**.
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**. Entrez l'adresse IP 0.0.0.0 s'il n'y a pas d'autre serveur DNS.
Enregistrer iDRAC sur DNS	Enregistre le nom iDRAC sur le serveur DNS.

	La valeur par défaut est **Désactivé**.
Nom iDRAC DNS	Affiche le nom iDRAC uniquement lorsque l'option **Enregistrer iDRAC sur DNS** est sélectionnée. Le nom par défaut est idrac-*numéro_de_service*, où *numéro_de_service* est le numéro de service du serveur Dell. Par exemple : idrac-00002.
Utiliser DHCP pour le nom de domaine DNS	Vous permet d'utiliser le nom de domaine DNS par défaut. Si la case n'est pas cochée et que l'option **Enregistrer iDRAC sur DNS** est sélectionnée, changez le nom de domaine DNS dans le champ **Nom de domaine DNS**. La valeur par défaut est **Désactivé**. **REMARQUE :** Pour cocher la case **Utiliser DHCP pour le nom de domaine DNS**, cochez également la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Nom de domaine DNS	Le champ du **nom de domaine DNS** par défaut est vide. Lorsque la case **Utiliser DHCP pour le nom de domaine DNS** est cochée, cette option est grisée et le champ ne peut pas être modifié.
Chaîne de communauté	Contient la chaîne de communauté à utiliser pour des interruptions d'alerte **SNMP (protocole de gestion de réseau simple)** envoyées à partir d'iDRAC. Les interruptions d'alerte SNMP sont transmises par iDRAC quand un événement sur plateforme se produit. La valeur par défaut est **public**.
Adresse du serveur SMTP	Adresse IP du serveur de **protocole simplifié de transfert de courrier (SMTP)** avec lequel iDRAC communique pour envoyer des alertes par e-mail lorsqu'un événement sur plateforme se produit. L'adresse par défaut est **127.0.0.1**.

Tableau 5-2. Paramètres LAN IPMI

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

Tableau 5-3. Boutons de la page Configuration réseau

Bouton	Description
Paramètres avancés	Ouvre la page **Sécurité réseau** pour permettre à l'utilisateur d'entrer les attributs de la plage IP et les attributs de blocage IP.
Imprimer	Imprime les valeurs de **Configuration réseau** qui apparaissent à l'écran.
Actualiser	Recharge la page **Configuration réseau**.
Appliquer	Enregistre les nouveaux paramètres définis sur la page Configuration réseau. **REMARQUE :** Les modifications des paramètres de l'adresse IP du NIC ferment toutes les sessions utilisateur et forcent les utilisateurs à se reconnecter à l'interface Web d'iDRAC avec les 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 du filtrage IP et du blocage IP

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

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

   Le tableau 5-4 décrit les paramètres de la page **Sécurité réseau**.
3. Une fois les paramètres configurés, cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-5.

Tableau 5-4. Paramètres de la page Sécurité réseau

Paramètres	Description
Plage IP activée	Active la fonctionnalité de vérification de la plage IP, qui définit une plage d'adresses IP pouvant accéder à iDRAC. La valeur par défaut est **désactivé**.
Adresse de la plage IP	Détermine l'adresse de sous-réseau IP autorisée. L'adresse par défaut est **192.168.1.0**.
Masque de sous-réseau de la plage IP	Définit les positions de bit significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau, où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur. L'adresse par défaut est **255.255.255.0**.

Blocage 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. La valeur par défaut est **désactivé**.
Nombre d'échecs avant blocage d'adresse IP	Définit le nombre d'échecs de tentatives de connexion à partir d'une adresse IP avant le rejet des tentatives de connexion à partir de cette adresse. L'adresse par défaut est **10**.
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. L'adresse par défaut est **3600**.
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. L'adresse par défaut est **3600.**

Tableau 5-5. Boutons de la page Sécurité réseau

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

Configuration des événements sur plateforme

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

Les événements sur plateforme pouvant être filtrés sont répertoriés dans le tableau 5-6.

Index	Événement sur plateforme
1	Assertion Avertissement batterie
2	Assertion batterie critique
3	Assertion Tension critique
4	Assertion Avertissement température
5	Assertion Température critique
6	Dégradation de la redondance
7	Perte de la redondance
8	Assertion Avertissement de processeur
9	Assertion Processeur critique
10	Assertion Processeur absent
11	Assertion Journal des événements critique
12	Assertion Surveillance critique

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

Si le même filtre d'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)

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

1. Connectez-vous à l'interface Web iDRAC. Voir Accès à l'interface Web.
2. Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.
3. Sur la page Événements sur plateforme, activez **Génération d'une alerte** pour un événement en cochant la case correspondante **Génération d'une alerte** pour cet événement.

REMARQUE : Vous pouvez activer ou désactiver la génération d'une alerte pour tous les événements en cliquant sur la case à cocher située en regard de l'en-tête de colonne Génération d'une alerte.

4. Cliquez sur le bouton radio sous l'action que vous voulez activer pour chaque événement. Une seule action peut être définie pour chaque événement.

5. Cliquez sur **Appliquer**.

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 des interruptions d'événement sur plateforme (PET)

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

1. Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge. Voir Accès à l'interface Web.
2. Assurez-vous d'avoir suivi les procédures décrites dans Configuration des filtres d'événements sur plateforme (PEF).
3. Configurez votre adresse IP de destination PET :
   a. Cliquez sur la case **Activer** à côté du **numéro de destination** que vous voulez activer.
   b. Saisissez une adresse IP dans la case **Adresse IP de destination**.

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

   c. Cliquez sur **Appliquer**.

   REMARQUE : Pour un envoi réussi d'une interruption, configurez la valeur de la **chaîne de communauté** sur la page **Configuration réseau**. La valeur **Chaîne de communauté** indique la chaîne de communauté à utiliser dans une interruption d'alerte SNMP (protocole de gestion de réseau simple) envoyée à partir d'iDRAC. Les interruptions d'alerte SNMP sont transmises par iDRAC quand un événement sur plateforme se produit. Le paramètre par défaut pour la **chaîne de communauté** est **Public**.

   d. Cliquez sur **Envoyer** pour tester l'alerte configurée (si nécessaire).
   e. Répétez les étapes a à d pour les autres numéros de destination.

Configuration des alertes par e-mail

1. Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge.
2. Assurez-vous d'avoir suivi les procédures décrites dans Configuration des filtres d'événements sur plateforme (PEF).
3. Configurez vos paramètres d'alerte par e-mail.
   a. Sur l'onglet **Gestion des alertes**, cliquez sur **Paramètres d'alertes par e-mail**.
4. Configurez votre destination d'alerte par e-mail.
   a. Dans la colonne **Numéro d'alerte par e-mail**, cliquez sur un numéro de destination. Il existe quatre destinations possibles pour recevoir des alertes.
   b. Assurez-vous que la case **Activé** est cochée.
   c. Dans le champ **Adresse e-mail de destination**, tapez une adresse e-mail valide.
   d. Cliquez sur **Appliquer**.

   REMARQUE : Pour réussir à envoyer un e-mail test, l'**adresse du serveur SMTP** doit être configurée sur la page **Configuration réseau**. L'adresse IP du **serveur SMTP** communique avec iDRAC pour envoyer des alertes par e-mail lorsqu'un événement sur plateforme se produit.

   e. Cliquez sur **Envoyer** pour tester l'alerte par e-mail configurée (si nécessaire).
   f. Répétez les étapes a à e pour les autres paramètres d'alerte par e-mail.

Configuration d'IPMI

1. Connectez-vous au système distant à l'aide d'un navigateur Web pris en charge.
2. Configurez IPMI sur le LAN.
   a. Cliquez sur **Système**→ **Accès à distance**→ iDRAC, puis cliquez sur l'onglet **Réseau/Sécurité**.
   b. Sur la page **Configuration réseau** sous **Paramètres LAN IPMI**, sélectionnez **Activer IPMI sur le LAN**.
   c. 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, voir 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**.

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

REMARQUE : L'interface IPMI iDRAC prend en charge le protocole RMCP+.

REMARQUE : La clé de cryptage doit se composer d'un nombre pair de caractères hexadécimaux d'un maximum de 20 caractères.

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

e. Cliquez sur **Appliquer**.

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

a. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**.

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

c. Sur la page **Configuration des communications série sur le LAN**, cochez la case **Activation des communications série sur le LAN** pour activer les 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 serveur géré.

Cliquez sur le menu déroulant **Débit en bauds** pour sélectionner une vitesse de données de 19,2 Kbits/s, 57,6 Kbits/s ou 115,2 Kbits/s.

e. Cliquez sur **Appliquer**.

Ajout et configuration des utilisateurs iDRAC

Pour gérer votre système avec iDRAC et maintenir la sécurité du système, créez des utilisateurs et octroyez-leur des droits d'administration spécifiques (*autorisation basée sur les rôles*).

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

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

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis cliquez sur l'onglet **Réseau/Sécurité**.

2. Ouvrez la page **Utilisateurs** pour configurer les utilisateurs.

   La page **Utilisateurs** affiche **la réf. utilisateur, l'état, le nom d'utilisateur, les privilèges LAN IPMI** de chaque utilisateur, les **privilèges iDRAC** et les **communications série sur le LAN**.

   REMARQUE : Utilisateur-1 est réservé pour l'utilisateur anonyme IPMI et n'est pas configurable.

3. Dans la colonne **Réf. utilisateur**, cliquez sur une référence utilisateur.

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

   Le tableau 5-7 décrit les paramètres **généraux** pour configurer un nom d'utilisateur et un mot de passe iDRAC.

   Le tableau 5-8 décrit les **privilèges LAN IPMI** pour configurer les privilèges LAN de l'utilisateur.

   Le tableau 5-9 décrit les droits de **groupe d'utilisateurs** pour les paramètres **Privilèges LAN IPMI** et **Privilèges utilisateur iDRAC**.

   Le tableau 5-10 décrit les droits du **groupe iDRAC**. Si vous ajoutez un **privilège utilisateur iDRAC** à **Administrateur**, **Utilisateur privilégié** ou **Utilisateur invité**, le **groupe iDRAC** bascule sur le groupe **Personnalisé**.

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

6. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-11.

Tableau 5-7. Propriétés générales

Propriété	Description
Réf. utilisateur	Contient l'un des 16 numéros d'utilisateur prédéfinis. Ce champ ne peut pas être modifié.

Activer l'utilisateur	Lorsqu'elle est cochée, cette propriété indique que l'accès de l'utilisateur à iDRAC est activé. Lorsqu'elle est décochée, l'accès utilisateur est désactivé.
Nom d'utilisateur	Spécifie un nom d'utilisateur iDRAC contenant jusqu'à 16 caractères. Chaque utilisateur doit avoir un nom d'utilisateur unique. **REMARQUE :** Les noms d'utilisateur iDRAC 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 ce champ est décoché, le **mot de passe** utilisateur ne peut pas être modifié.
Nouveau mot de passe	Active la modification du mot de passe de l'utilisateur iDRAC. Entrez un **mot de passe** de 20 caractères au maximum. Les caractères ne seront pas affichés.
Confirmez le nouveau mot de passe	Retapez le mot de passe de l'utilisateur iDRAC pour le confirmer.

Tableau 5-8. Privilèges utilisateur sur le LAN IPMI

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

Tableau 5-9. Privilèges utilisateur iDRAC

Propriété	Description
Groupe iDRAC	Spécifie le privilège utilisateur iDRAC maximum sur l'une des options suivantes : **Administrateur**, **Utilisateur privilégié**, **Utilisateur invité**, **Personnalisé** ou **Aucun**. Voir le tableau 5-10 pour accéder aux droits du **groupe iDRAC**.
Ouvrir une session iDRAC	Permet à l'utilisateur d'ouvrir une session iDRAC.
Configurer iDRAC	Permet à l'utilisateur de configurer iDRAC.
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 iDRAC.
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 5-10. Droits du groupe iDRAC

Groupe d'utilisateurs	Droits accordés
Administrateur	**Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**
Utilisateur privilégié	**Ouverture de session iDRAC**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**
Invité	**Ouvrir une session iDRAC**
Personnalisé	Sélectionne parmi les autorisations suivantes : **Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes d'action du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**
Aucune	Aucun droit attribué

Tableau 5-11. Boutons de la page Configuration utilisateur

Bouton	Action
Imprimer	Imprime les valeurs de **Configuration utilisateur** qui apparaissent à l'écran.

Actualiser	Recharge la page **Configuration utilisateur**.
Appliquer	Enregistre les nouveaux paramètres définis pour la configuration utilisateur.
Retour à la page Utilisateurs	Retourne à la page **Utilisateurs**.

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

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

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

Protocole Secure Sockets Layer (SSL)

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

Un système compatible SSL peut effectuer les tâches suivantes :

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

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

Requête de signature de certificat (RSC)

Une RSC est une demande numérique adressée à une autorité de certification pour un certificat de serveur sécurisé. Les certificats de serveur sécurisés permettent aux clients du serveur de faire confiance à l'identité du serveur auquel ils se sont connectés et de négocier une session cryptée avec le serveur.

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

Une fois que l'autorité de certification approuve la RSC et qu'elle envoie le certificat, téléversez ce dernier sur le micrologiciel iDRAC. Les informations de la RSC enregistrées sur le micrologiciel iDRAC doivent correspondre aux informations du certificat.

Accès au menu principal SSL

1. Cliquez sur **Système**→ **Accès à distance** → **iDRAC**, puis cliquez sur l'onglet **Réseau/Sécurité**.
2. Cliquez sur **SSL** pour ouvrir la page **Menu principal SSL**.

Utilisez la page **Menu principal SSL** pour générer une RSC à envoyer à une autorité de certification. Les informations de la RSC sont stockées dans le micrologiciel iDRAC.

Le tableau 5-12 décrit les options disponibles lors de la génération d'une RSC.

Le tableau 5-13 décrit les boutons disponibles sur la page **Menu principal SSL**.

Tableau 5-12. Options du menu principal SSL

Champ	Description
Générer une nouvelle requête de	Sélectionnez l'option et cliquez sur **Suivant** pour ouvrir la page **Générer une requête de signature de certificat**

signature de certificat (RSC)	**(RSC)**. **REMARQUE :** La nouvelle RSC remplace toujours la RSC présente sur le micrologiciel. Pour qu'une autorité de certification accepte votre RSC, la RSC du micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification.
Téléverser le certificat de serveur	Sélectionnez l'option et cliquez sur **Suivant** pour ouvrir la page **Téléversement d'un certificat** et téléverser le certificat que vous a envoyé l'autorité de certification. **REMARQUE :** iDRAC n'accepte que les certificats X509, encodés en base 64. Les certificats encodés DER ne sont pas acceptés.
Afficher le certificat de serveur	Sélectionnez l'option et cliquez sur **Suivant** pour ouvrir la page **Afficher le certificat de serveur** et afficher un certificat de serveur existant.

Tableau 5-13. Boutons du menu principal SSL

Bouton	Description
Imprimer	Imprime les valeurs de **Menu principal SSL** qui apparaissent à l'écran.
Actualiser	Recharge la page **Menu principal SSL**.
Suivant	Traite les informations sur la page **Menu principal SSL** et passe à la prochaine étape.

Génération d'une nouvelle requête de signature de certificat

REMARQUE : La nouvelle RSC remplace toujours les données de RSC stockées sur le micrologiciel. La RSC présente dans le micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification. Sinon, iDRAC n'acceptera pas le certificat.

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

   Le tableau 5-14 décrit les options de la page **Générer une requête de signature de certificat (RSC)**.
3. Cliquez sur **Générer** pour créer la requête de signature de certificat.
4. Cliquez sur **Télécharger** pour enregistrer le fichier RSC sur votre ordinateur local.
5. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-15.

Tableau 5-14. Options de la page Générer une requête de signature de certificat (RSC)

Champ	Description
Nom de domaine	Le nom exact à certifier (normalement, le nom de domaine du serveur Web comme, par exemple, **www.compagniexyz.com**). Seuls les caractères alphanumériques, les tirets, les traits de soulignement et les points sont valides. Les espaces ne sont pas valides.
Nom de la 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, Informatique). 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.
Indicatif du pays	Le nom du pays où se trouve la compagnie qui demande la certification.
E-mail	Adresse e-mail associée à la RSC. Tapez l'adresse e-mail de l'entreprise ou toute autre adresse e-mail associée à la RSC. Ce champ est optionnel.

Tableau 5-15. Boutons de la page Générer une requête de signature de certificat (RSC)

Bouton	Description
Imprimer	Imprime les valeurs de **Générer une requête de signature de certificat** qui apparaissent à l'écran.
Actualiser	Recharge la page **Générer une requête de signature de certificat**.
Générer	Génère une RSC et invite l'utilisateur à l'enregistrer dans un répertoire spécifié.
Télécharger	Télécharge le certificat sur l'ordinateur local.

Retour au menu principal SSL	Renvoie l'utilisateur à la page **Menu principal SSL**.

Téléversement d'un certificat de serveur

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

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

2. Dans le champ **Chemin de fichier**, tapez le chemin d'accès au certificat ou cliquez sur **Parcourir** pour naviguer jusqu'au fichier de certificat.

REMARQUE : La valeur **Chemin d'accès au fichier** affiche le chemin d'accès au fichier relatif au certificat que vous téléversez. 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 pour continuer. Voir tableau 5-16.

Tableau 5-16. Boutons de la page Téléversement d'un certificat

Bouton	Description
Imprimer	Imprime les valeurs qui apparaissent sur la page **Téléversement d'un certificat**.
Actualiser	Recharge la page **Téléversement d'un certificat**.
Appliquer	Applique le certificat au micrologiciel iDRAC.
Retour au menu principal SSL	Renvoie l'utilisateur à la page **Menu principal SSL**.

Affichage d'un certificat de serveur

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

   Le tableau 5-17 décrit les champs et les descriptions associées répertoriés dans la fenêtre **Certificat**.

2. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-18.

Tableau 5-17. 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 5-18. Boutons de la page Afficher le certificat de serveur

Bouton	Description
Imprimer	Imprime les valeurs de **Afficher le certificat de serveur** qui apparaissent à l'écran.
Actualiser	Recharge la page **Afficher le certificat de serveur**.
Retour au menu principal SSL	Retourne à la page **Menu principal SSL**.

Configuration et gestion des certificats Active Directory

REMARQUE : Vous devez avoir le droit de **configurer iDRAC** pour configurer Active Directory et téléverser, 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 un schéma étendu, voir Utilisation d'iDRAC avec Microsoft Active Directory.

Pour accéder au **menu principal d'Active Directory** :

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC,** puis cliquez sur l'onglet **Réseau/Sécurité**.
2. Cliquez sur **Active Directory** pour ouvrir la page **Menu principal d'Active Directory**.

   Le tableau 5-19 répertorie les options de la page **Menu principal d'Active Directory**.
3. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-20.

Tableau 5-19. Options de la page Menu principal d'Active Directory

Champ	Description
Configurer Active Directory	Configure le **nom de domaine racine** d'Active Directory, le **délai d'attente de l'authentification d'Active Directory**, la **sélection du schéma d'Active Directory**, le **nom iDRAC**, le **nom de domaine iDRAC**, les **groupes de rôles**, le **nom du groupe** et les **paramètres du domaine du groupe**.
Téléverser le certificat d'autorité de certification d'Active Directory	Téléverse un certificat Active Directory sur iDRAC.
Télécharger un certificat de serveur iDRAC	Le **gestionnaire de téléchargement Windows** télécharge un certificat de serveur iDRAC sur le système.
Afficher le certificat d'autorité de certification d'Active Directory	Affiche un certificat Active Directory qui a été téléversé sur iDRAC.

Tableau 5-20. Boutons de la page Menu principal d'Active Directory

Bouton	Définition
Imprimer	Imprime les valeurs du **menu principal d'Active Directory** apparaissant à l'écran.
Actualiser	Recharge la page **Menu principal d'Active Directory**.
Suivant	Traite les informations de la page **Menu principal d'Active Directory** et passe à l'étape suivante.

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 d'Active Directory**, entrez les paramètres Active Directory.

   Le tableau 5-21 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 pour continuer. Voir tableau 5-22.
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 5-23 et tableau 5-24.

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

Tableau 5-21. Paramètres de la page Configuration d'Active Directory

Paramètre	Description
Activer Active Directory	Lorsqu'il est coché, active Active Directory. **Désactivé** est sélectionné par défaut.
Nom de domaine racine	Le nom de domaine racine d'Active Directory. Cette valeur par défaut est blanc. 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 ou org. La valeur par défaut est blanc.
Délai d'attente	Le délai écoulé, en secondes, nécessaire pour que les requêtes d'Active Directory puissent se terminer. La valeur minimale est supérieure ou égale à 15 secondes. La valeur par défaut est **120**.
Utiliser le schéma standard	Utilise le schéma standard avec Active Directory.
Utiliser le schéma	Utilise le schéma étendu avec Active Directory.

étendu	
Nom iDRAC	Nom qui identifie de manière exclusive iDRAC dans Active Directory. Cette valeur par défaut est blanc. Le nom doit être une chaîne de 1 à 254 caractères ASCII, sans espace entre les caractères.
Nom de domaine iDRAC	Nom DNS du domaine où l'objet Active Directory iDRAC réside. Cette valeur par défaut est blanc. 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 ou org.
Groupe de rôles	Liste des groupes de rôles associés à iDRAC. Pour changer les paramètres d'un groupe de rôles, cliquez sur son numéro dans la liste des groupes de rôles.
Nom du groupe	Nom qui identifie le groupe de rôles d'Active Directory associé à iDRAC. Cette valeur par défaut est blanc.
Domaine du groupe	Type de domaine où le groupe de rôles réside.

Tableau 5-22. Boutons de la page Configuration d'Active Directory

Bouton	Description
Imprimer	Imprime les valeurs de **Configuration d'Active Directory** qui apparaissent à l'écran.
Actualiser	Recharge la page **Configuration d'Active Directory**.
Appliquer	Enregistre les nouveaux paramètres définis sur la page **Configuration d'Active Directory**.
Retour au menu principal d'Active Directory	Retourne à la page **Menu principal d'Active Directory**.

Tableau 5-23. Privilèges de groupes de rôles

Paramètre	Description
Niveau de privilèges du groupe de rôles	Spécifie le privilège utilisateur iDRAC maximum de l'utilisateur sur l'une des options suivantes : **Administrateur**, **Utilisateur privilégié**, **Utilisateur invité**, **Aucun** ou **Personnalisé**. Voir le tableau 5-24 pour accéder aux droits des **groupes de rôles**.
Ouvrir une session iDRAC	Permet au groupe d'ouvrir une session pour accéder à iDRAC.
Configurer iDRAC	Permet au groupe de configurer iDRAC.
Configuration des utilisateurs	Permet au groupe de configurer des utilisateurs.
Effacer les journaux	Permet au groupe d'effacer des journaux.
Exécution des commandes de contrôle du serveur	Permet au groupe d'exécuter des commandes de contrôles du serveur.
Accès à la redirection de console	Permet au groupe d'accéder à la redirection de console.
Accès au média virtuel	Permet au groupe d'accéder au média virtuel.
Tester les alertes	Permet au groupe d'envoyer des alertes d'essai (e-mail et PET) à un utilisateur spécifique.
Exécution des commandes de diagnostic	Permet au groupe d'exécuter des commandes de diagnostics.

Tableau 5-24. Droits des groupes de rôles

Propriété	Description
Administrateur	**Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**
Utilisateur privilégié	**Ouverture de session iDRAC**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**
Invité	**Ouvrir une session iDRAC**
Personnalisé	Sélectionne parmi les autorisations suivantes : **Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes d'action du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**
Aucune	Aucun droit attribué

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

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Téléverser le certificat d'autorité de certification d'Active Directory** et cliquez sur **Suivant**.

2. Sur la page **Téléversement 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 téléversez. 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.

Vérifiez que les certificats SSL du contrôleur de domaine sont signés par la même autorité de certification et que ce certificat est disponible sur la station de gestion accédant à iDRAC.

3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-25.

Tableau 5-25. Boutons de la page Téléversement d'un certificat

Bouton	Description
Imprimer	Imprime les valeurs de **Téléversement d'un certificat** apparaissant à l'écran.
Actualiser	Recharge la page **Téléversement d'un certificat**.
Appliquer	Applique le certificat au micrologiciel iDRAC.
Retour au menu principal d'Active Directory	Retourne à la page **Menu principal d'Active Directory**.

Téléchargement d'un certificat de serveur iDRAC

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Télécharger un certificat de serveur iDRAC** et cliquez sur **Suivant**.
2. 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 iDRAC.

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 5-26 décrit les champs et les descriptions associées répertoriés dans la fenêtre **Certificat**.
2. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-27.

Tableau 5-26. 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 5-27. Boutons de la page Afficher le certificat d'autorité de certification d'Active Directory

Bouton	Description
Imprimer	Imprime les valeurs de **Certificat d'autorité de certification d'Active Directory apparaissant à l'écran**.
Actualiser	Recharge la **page Certificat d'autorité de certification d'Active Directory**.
Retour au menu principal d'Active Directory	Renvoie l'utilisateur à la page **Menu principal d'Active Directory**.

Configuration des communications série sur le LAN

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**.

2. Cliquez sur **Communications série sur le LAN** pour ouvrir la page **Configuration des communications série sur le LAN**.

   Le tableau 5-28 fournit des informations sur les paramètres de la page **Configuration des communications série sur le LAN**.

3. Cliquez sur **Appliquer**.

4. Configurez les paramètres avancés, si nécessaire. Sinon, cliquez sur le bouton approprié pour continuer. Voir tableau 5-29.

   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 5-30.

   c. Cliquez sur **Appliquer**.

   d. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-31.

Tableau 5-28. Paramètres de la page Configuration des communications série sur le LAN

Paramètre	Description
Activation des connexions série sur le LAN	Lorsqu'elle est cochée, cette case indique que les communications série sur le LAN sont activées.
Débit en bauds	Indique la vitesse de transmission des données. Sélectionnez une vitesse de données de **19,2 Kbits/s**, **57,6 Kbits/s** ou **115,2 Kbits/s**.

Tableau 5-29. Boutons de la page Configuration des communications série sur le LAN

Bouton	Description
Imprimer	Imprime les valeurs de **Configuration des communications série sur le LAN** qui apparaissent à l'écran.
Actualiser	Recharge 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	Fournit les nouveaux paramètres que vous créez lors de l'affichage de la page **Configuration des communications série sur le LAN**.

Tableau 5-30. Paramètres de la page Paramètres avancés de la configuration des communications série sur le LAN

Paramètre	Description
Intervalle d'accumulation des caractères	Le délai qu'iDRAC doit respecter avant de transmettre un paquet partiel de données de caractères SOL. Le délai est mesuré en secondes.
Seuil d'envoi des caractères	iDRAC envoie un paquet de données de caractères SOL, contenant les caractères dès que ce nombre de caractères (ou un nombre supérieur) a été accepté. Le seuil est mesuré en caractères.

Tableau 5-31. Boutons de la page Paramètres avancés de la configuration des communications série sur le LAN

Bouton	Description
Imprimer	Imprime les valeurs de **Paramètres avancés de la configuration des communications série sur le LAN** qui apparaissent à l'écran.
Actualiser	Recharge la page **Paramètres avancés de la configuration des communications série sur le LAN**.
Appliquer	Enregistre les nouveaux paramètres que vous créez pendant l'affichage de **Paramètres avancés de la configuration des communications série sur le LAN**.
Retour à la page Configuration des communications série sur le LAN	Renvoie l'utilisateur à la page **Configuration des communications série sur le LAN**.

Configuration des services iDRAC

REMARQUE : Pour modifier ces paramètres, vous devez avoir le droit de **configurer iDRAC**.

REMARQUE : Lorsque vous appliquez les changements aux services, ceux-ci prennent effet immédiatement. Les connexions existantes peuvent prendre fin sans avertissement.

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis cliquez sur l'onglet **Réseau/Sécurité**.

2. Cliquez sur **Services** pour ouvrir la page de configuration **Services**.

3. Configurez les services suivants, si nécessaire :
   - Web Server : voir le tableau 5-32 pour accéder aux paramètres Web Server
   - SSH : voir le tableau 5-33 pour accéder aux paramètres SSH
   - Telnet : voir le tableau 5-34 pour accéder aux paramètres Telnet
   - Agent de récupération automatique du système : voir le tableau 5-35 pour accéder aux paramètres de l'agent de récupération automatique du système
4. Cliquez sur **Appliquer**.
5. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-36.

Tableau 5-32. Paramètres de Web Server

Paramètre	Description
Activé	Active ou désactive le serveur Web iDRAC. Lorsqu'elle est cochée, cette case indique que Web Server est activé. **Activé** est sélectionné par défaut.
Nombre maximal de sessions	Nombre maximum de sessions simultanées autorisées pour ce système. Ce champ ne peut pas être modifié. Quatre sessions peuvent être exécutées simultanément.
Sessions ouvertes	Nombre de sessions actuelles sur le système, inférieur ou égal à **Nombre maximal de sessions**. Ce champ ne peut pas être modifié.
Délai d'attente	Durée, en secondes, pendant laquelle une connexion peut rester inactive. La session est annulée quand le délai d'attente est atteint. Les modifications apportées au paramètre de délai d'attente prennent effet immédiatement et réinitialisent Web Server. La plage du délai d'attente est comprise entre 60 et 1920 secondes. La valeur par défaut est **300** secondes.
Numéro de port HTTP	Port sur lequel iDRAC écoute une connexion au navigateur. L'adresse par défaut est **80**.
Numéro de port HTTPS	Port sur lequel iDRAC écoute une connexion au navigateur sécurisée. L'adresse par défaut est **443**.

Tableau 5-33. Paramètres SSH

Paramètre	Description
Activé	Active ou désactive SSH. Lorsqu'elle est cochée, cette case indique que SSH est activé.
Nombre maximal de sessions	Nombre maximum de sessions simultanées autorisées pour ce système. Une seule session est prise en charge.
Sessions actives	Nombre de sessions ouvertes sur le système.
Délai d'attente	Délai d'attente Secure Shell, en secondes. La plage du délai d'attente est comprise entre 60 et 1920 secondes. Entrez 0 seconde pour désactiver le fonctionnalité de délai d'attente. L'adresse par défaut est **300**.
Numéro de port	Port sur lequel iDRAC écoute une connexion SSH. L'adresse par défaut est **22**.

Tableau 5-34. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé.
Nombre maximal de sessions	Nombre maximum de sessions simultanées autorisées pour ce système. Une seule session est prise en charge.
Sessions actives	Nombre de sessions ouvertes sur le système.
Délai d'attente	Délai d'attente en cas d'inactivité de la commande telnet, en secondes. La plage du délai d'attente est comprise entre 60 et 1920 secondes. Entrez 0 seconde pour désactiver le fonctionnalité de délai d'attente. L'adresse par défaut est **0**.
Numéro de port	Port sur lequel iDRAC écoute une connexion Telnet. L'adresse par défaut est **23**.

Tableau 5-35. Paramètre de l'agent de récupération automatique du système

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

Tableau 5-36. Boutons de la page Services

Bouton	Description
Imprimer	Imprime la page **Services**.
Actualiser	Actualise la page **Services**.

Appliquer les changements	Applique les paramètres de la page **Services**.

Mise à jour du micrologiciel iDRAC

AVIS : Si le micrologiciel iDRAC devient corrompu, ce qui peut être le cas lorsque la progression de la mise à jour du micrologiciel iDRAC est interrompue avant qu'elle ne se termine, vous pouvez récupérer iDRAC à l'aide de CMC. Consultez votre *Guide d'utilisation du micrologiciel CMC* pour obtenir des instructions.

REMARQUE : Par défaut, la mise à jour du micrologiciel conserve les paramètres iDRAC définis. Lors du processus de mise à jour, vous avez la possibilité de rétablir les paramètres d'usine de la configuration iDRAC. Si vous rétablissez les paramètres d'usine de la configuration, l'accès réseau externe sera désactivé une fois la mise à jour terminée. Vous devez activer et configurer le réseau à l'aide de l'utilitaire de configuration iDRAC ou via l'interface Web CMC.

1. Démarrez l'interface Web iDRAC.
2. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis cliquez sur l'onglet **Mise à jour**.

   REMARQUE : Pour mettre à jour le micrologiciel, iDRAC doit mis en mode de mise à jour. Lorsqu'il se trouve sur ce mode, iDRAC se réinitialise automatiquement, même si vous annulez le processus de mise à jour.
3. Sur la page **Mise à jour de micrologiciel**, cliquez sur **Suivant** pour démarrer le processus de mise à jour.
4. Dans la fenêtre **Mise à jour de micrologiciel - Téléversement (page 1 sur 4)**, cliquez sur **Parcourir** ou tapez le chemin d'accès à l'image de micrologiciel que vous avez téléchargée.

   Par exemple :

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

   Par défaut, le nom de l'image du micrologiciel est **firmimg.imc**.
5. Cliquez sur **Suivant**.
   - Le fichier va se téléverser sur iDRAC. Cette opération peut prendre quelques minutes.

     OU
   - Cliquez sur **Annuler** à cet instant pour arrêter le processus de mise à niveau du micrologiciel. Si vous cliquez sur **Annuler,** iDRAC revient au mode de fonctionnement normal.
6. Dans la fenêtre **Mise à jour de micrologiciel - Validation (étape 2 sur 4)**, vous pouvez voir les résultats de la validation effectuée sur le fichier image téléversé.
   - Si le fichier image s'est téléversé et a réussi toutes les vérifications, un message apparaît indiquant que l'image du micrologiciel a été vérifiée.

     OU
   - Si l'image ne s'est pas téléversée ou n'a pas réussi les vérifications, la mise à jour de micrologiciel retourne à la fenêtre **Mise à jour de micrologiciel - Téléversement (page 1 sur 4)**. Vous pouvez réessayer de mettre à niveau iDRAC ou cliquer sur **Annuler** pour faire revenir iDRAC au mode de fonctionnement normal.

   REMARQUE : Si vous décochez la case **Préserver la configuration**, les paramètres par défaut d'iDRAC seront rétablis. Dans les paramètres par défaut, le LAN est désactivé. Vous ne pourrez pas vous connecter à l'interface Web iDRAC. Vous devrez reconfigurer les paramètres LAN via l'interface Web CMC ou iKVM à l'aide de l'utilitaire de configuration iDRAC lors du POST du BIOS.
7. Par défaut, la case **Préserver la configuration** est cochée pour conserver les paramètres iDRAC définis après une mise à niveau. Si vous ne voulez pas que les paramètres soient préservés, désélectionnez la case à cocher **Préserver la configuration**.
8. Cliquez sur **Démarrer la mise à jour** pour démarrer le processus de mise à niveau. N'interrompez pas le processus de mise à niveau.
9. Dans la fenêtre **Mise à jour de micrologiciel - Mise à jour (étape 3 sur 4)**, la condition de la mise à niveau est affichée. La progression de l'opération de mise à niveau de micrologiciel, indiquée en pourcentage, apparaît dans la colonne **Progression**.
10. Une fois la mise à jour de micrologiciel terminée, la fenêtre **Mise à jour de micrologiciel - Résultats de la mise à jour (page 4 sur 4)** apparaît et iDRAC se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC avec une nouvelle fenêtre de navigateur.

Récupération du micrologiciel iDRAC à l'aide de CMC

Généralement, le micrologiciel iDRAC est mis à jour à l'aide des services iDRAC, comme par exemple l'interface Web iDRAC, l'interface de ligne de commande SM-CLP ou les progiciels de mise à jour spécifiques au système d'exploitation téléchargés à l'adresse **support.dell.com**.

Si le micrologiciel iDRAC devient corrompu, ce qui peut être le cas lorsque la progression de la mise à jour du micrologiciel iDRAC est interrompue avant qu'elle ne se termine, vous pouvez utiliser l'interface Web CMC pour mettre à jour son micrologiciel.

Si CMC détecte le micrologiciel iDRAC corrompu, iDRAC est répertorié sur la page **Composants pouvant être mis à jour** dans l'interface Web CMC.

REMARQUE : Voir le *Guide d'utilisation du micrologiciel CMC* pour obtenir des instructions relatives à l'utilisation de l'interface Web CMC.

Pour mettre à jour le micrologiciel iDRAC, effectuez les étapes suivantes :

1. Téléchargez la dernière version du micrologiciel iDRAC sur votre ordinateur de gestion depuis l'adresse **support.dell.com**.
2. Connectez-vous à l'interface Web CMC.
3. Cliquez sur **Châssis dans l'arborescence du système**.
4. Cliquez sur l'onglet **Mise à jour**. La page **Composants pouvant être mis à jour** apparaît. Le serveur incluant l'iDRAC récupérable est inclus dans la liste s'il peut être récupéré à partir de CMC.
5. Cliquez sur **serveur-*n***, où ***n*** est le numéro du serveur dont vous souhaitez récupérer l'iDRAC.
6. Cliquez sur **Parcourir** pour accéder à l'image de micrologiciel iDRAC que vous avez téléchargé, puis cliquez sur **Ouvrir**.
7. Cliquez sur **Commencer la mise à jour de micrologiciel**.

Une fois le fichier image de micrologiciel téléversé sur CMC, iDRAC se met à jour avec l'image.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation d'iDRAC avec Microsoft Active Directory

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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 et des autres périphériques d'un réseau. Si votre société utilise le logiciel de service Microsoft® Active Directory®, il peut être configuré pour vous donner accès à iDRAC et vous permettre d'ajouter et de contrôler les privilèges utilisateur iDRAC pour les utilisateurs présents dans votre logiciel Active Directory.

REMARQUE : L'utilisation d'Active Directory pour reconnaître les utilisateurs iDRAC 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 à iDRAC via une solution de schéma étendu qui utilise des objets Active Directory définis par Dell ou via une solution de schéma standard qui n'utilise que des objets du groupe d'Active Directory.

Avantages et inconvénients des schémas étendu et standard

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

L'utilisation de la solution du schéma étendu a les avantages suivants :

- Tous les objets de contrôle de l'accès sont contenus dans Active Directory.
- La configuration de l'accès utilisateur sur des iDRAC ayant des niveaux de privilège différents est très flexible.

L'utilisation de la solution du schéma standard présente les avantages suivants :

- Aucune extension de schéma n'est nécessaire parce que le schéma standard n'utilise que des objets Active Directory.
- La configuration d'Active Directory est aisée.

Présentation du schéma étendu d'Active Directory

Vous pouvez activer Active Directory avec le schéma étendu de trois manières :

- Avec l'interface Web iDRAC. Voir Configuration d'iDRAC avec le schéma étendu d'Active Directory via l'interface Web
- Avec l'outil CLI RACADM. Voir Configuration d'iDRAC avec le schéma étendu d'Active Directory via RACADM.
- Avec la ligne de commande SM-CLP. Voir Configuration d'iDRAC avec le schéma étendu d'Active Directory et SM-CLP

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 attributs et les classes 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 identificateur exclusif. Pour que les identificateurs 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 dans Microsoft Active Directory, Dell a reçu des identificateurs d'objets uniques, des extensions de noms uniques et des références d'attributs liées de façon unique pour les attributs et classes ayant été ajoutés au service d'annuaire, comme illustré dans le tableau 6-1.

Tableau 6-1. Identificateurs d'objets Dell Active Directory

Classe de service Active Directory	Identificateurs d'objets Active Directory
Extension Dell	dell
Identificateurs d'objets de base Dell	1.2.840.113556.1.8000.1280
Plage de numéro du lien RAC	12070 à 12079

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

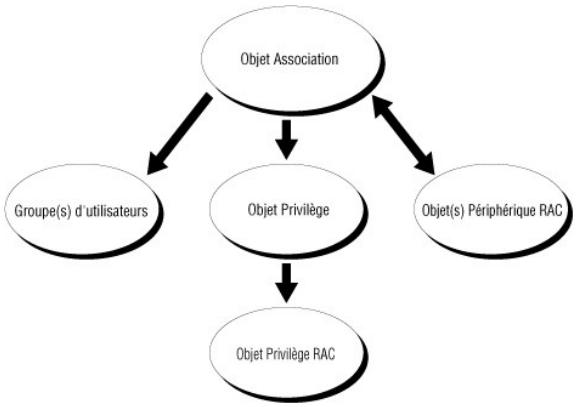
Pour chacun des RAC physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, vous devez créer au moins un objet Association et un objet Périphériques RAC. Vous pouvez créer autant d'objets Association que vous le voulez, et chaque 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 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. L'administrateur doit ajouter 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 iDRAC.

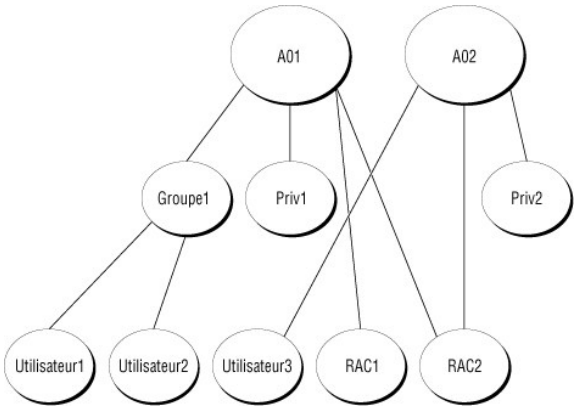
Vous pouvez créer autant d'objets Association que vous le voulez. Cependant, vous devez créer au moins un objet Association et vous devez avoir un objet Périphérique RAC pour chaque RAC (iDRAC) du réseau que vous voulez intégrer à Active Directory pour en gérer l'authentification et l'autorisation.

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.

Vous pouvez configurer des objets Active Directory dans un domaine unique ou dans des domaines multiples. Par exemple, supposons que vous avez deux iDRAC (RAC1 et RAC2) et trois utilisateurs Active Directory (utilisateur1, utilisateur2 et utilisateur3). Vous voulez accorder des privilèges d'administrateur à utilisateur1 et à utilisateur2 sur les deux iDRAC et des privilèges d'ouverture de session à utilisateur3 sur 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



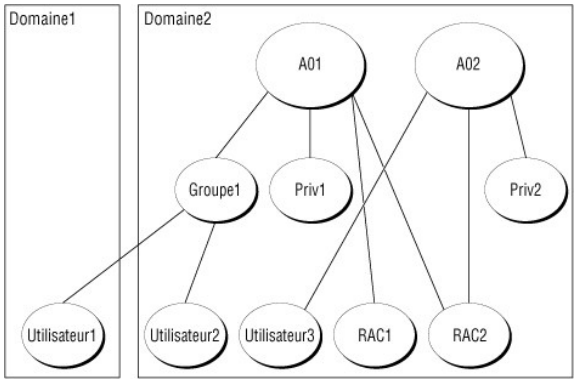
Pour configurer les objets pour le scénario de domaine unique, effectuez les tâches suivantes :

1. Créez deux objets Association.
2. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux iDRAC.
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 (AO1), Priv1 comme objets Privilèges dans AO1 et RAC1 et RAC2 comme périphériques RAC dans AO1.
6. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (AO2), Priv2 comme objets Privilèges dans AO2 et RAC2 comme périphériques RAC dans AO2.

Voir Ajout d'utilisateurs iDRAC et de leurs privilèges 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 iDRAC (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 iDRAC et configurez utilisateur3 avec les droits d'ouverture de session sur 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, AO1 (d'étendue Universel) et AO2, 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 iDRAC.
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 à iDRAC

Pour pouvoir utiliser Active Directory pour accéder à iDRAC, configurez le logiciel Active Directory et iDRAC en effectuant les étapes suivantes dans l'ordre :

1. Étendez le schéma d'Active Directory (voir Extension du schéma d'Active Directory).

2. Étendez le snap-in Utilisateurs et ordinateurs Active Directory (voir Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory).

3. Ajoutez les utilisateurs iDRAC et leurs privilèges à Active Directory (voir Ajout d'utilisateurs iDRAC et de leurs privilèges à Active Directory).

4. Activez SSL sur tous vos contrôleurs de domaine (voir Activation de SSL sur un contrôleur de domaine).

5. Configurez les propriétés Active Directory iDRAC via l'interface Web iDRAC ou RACADM (voir Configuration d'iDRAC avec le schéma étendu d'Active Directory via l'interface Web ou Configuration d'iDRAC avec le schéma étendu d'Active Directory via 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 soit :

- Utilitaire Dell Schema Extender
- 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 :

- *Lecteur de CD* **:\support\omactivedirectory tools\rac4-5\ldif_files**
- *Lecteur de CD* **:\support\omactivedirectory tools\rac4-5\schema_extender**

Pour utiliser les fichiers LDIF, voir les 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, voir 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 comprenez 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 :

   - Classes (voir tableau 6-2 à tableau 6-7)
   - Attributs (tableau 6-8)

   Consultez votre documentation Microsoft pour des informations supplémentaires sur la façon d'activer et d'utiliser le snap-in du schéma Active Directory de MMC.

Tableau 6-2. 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 6-3. Classe dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Description	Représente le périphérique RAC de Dell. Le périphérique RAC doit être configuré en tant que dellRacDevice dans Active Directory. Cette configuration permet à iDRAC 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 6-4. Classe dellAssociationObject

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

Tableau 6-5. Classe dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Permet de définir les privilèges (droits d'autorisation) du périphérique iDRAC.
Type de classe	Classe auxiliaire
SuperClasses	Aucun
Attributs	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tableau 6-6. Classe dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Fait office de classe de conteneurs pour les privilèges Dell (Droits d'autorisation).
Type de classe	Classe structurelle
SuperClasses	Utilisateur
Attributs	dellRAC4Privileges

Tableau 6-7. Classe dellProduct

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

Tableau 6-8. Liste des attributs ajoutés au schéma 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)	FAUX
dellProductMembers Liste des objets dellRacDevices appartenant à ce rôle. Cet attribut est le lien suivant qui correspond au lien dellAssociationMembers précédent. Numéro 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)	FAUX
dellIsLoginUser VRAI 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)	VRAI
dellIsCardConfigAdmin VRAI 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)	VRAI
dellIsUserConfigAdmin VRAI 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)	VRAI
dellIsLogClearAdmin VRAI 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)	VRAI
dellIsServerResetUser VRAI 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)	VRAI
dellIsConsoleRedirectUser VRAI 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)	VRAI
dellIsVirtualMediaUser VRAI 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)	VRAI
dellIsTestAlertUser VRAI 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)	VRAI
dellIsDebugCommandAdmin VRAI 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)	VRAI
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 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VRAI
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 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VRAI
dellAssociationMembers Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien précédent vers l'attribut lié dellProductMembers. Numéro du lien : 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FAUX

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 (iDRAC), les utilisateurs et les groupes d'utilisateurs, les associations de RAC et les privilèges de RAC.

Lorsque vous installez Systems Management Software 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. Voir 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 iDRAC d'Active Directory. Si vous n'installez pas le pack administrateur, vous ne pouvez pas visualiser l'objet RAC Dell dans le conteneur.

Voir 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**→ **Utilisateurs et Ordinateurs Active Directory**.

   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 iDRAC et de leurs privilèges à Active Directory

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

- Créez un objet Périphérique RAC
- Créez un objet Privilège
- Créez un objet Association
- Ajoutez des objets à un objet Association

Création d'un objet Périphérique RAC

1. Dans la fenêtre **Racine de la console** MMC, cliquez-droite sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet RAC Dell**.

   La fenêtre **Nouvel objet** apparaît.

3. Tapez le nom du nouvel objet. Le nom doit être le même que le nom iDRAC que vous tapez à l'étape a de la section Configuration d'iDRAC avec le schéma étendu d'Active Directory via 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, voir Privilèges utilisateur iDRAC).

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 d'iDRAC avec le schéma étendu d'Active Directory via l'interface Web

1. Ouvrez une fenêtre de navigateur Web prise en charge.
2. Connectez-vous à l'interface Web iDRAC.
3. Cliquez sur **Système**→ **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 (voir l'étape 3 de la section « Création d'un objet Périphérique RAC »).
   b. Tapez le **nom de domaine DRAC** (par exemple, `iDRAC.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. Téléversez votre certificat d'autorité de certification racine de forêt de domaine dans iDRAC.
    a. Sélectionnez le bouton radio **Téléverser le certificat d'autorité de certification d'Active Directory**, puis cliquez sur **Suivant**.
    b. Sur la page **Téléversement 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 téléversez. 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 accédant à iDRAC (voir Exportation d'un certificat d'autorité de certification racine du contrôleur de domaine).

    c. Cliquez sur **Appliquer**.

    Le serveur Web iDRAC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
12. Fermez puis ouvrez une session iDRAC pour terminer la configuration de la fonctionnalité Active Directory iDRAC.
13. Cliquez sur **Système**→ **Accès à distance**.

14. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.

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 du schéma étendu d'Active Directory iDRAC est terminée.

Configuration d'iDRAC avec le schéma étendu d'Active Directory via RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory avec le schéma étendu iDRAC via l'outil de l'interface de ligne de commande 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 <FQDN rac>

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <FQDN racine>

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

   racadm sslcertupload -t 0x2 -f <URI TFTP du certificat d'autorité de certification racine>

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

2. Si DHCP est activé sur iDRAC 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 iDRAC ou que vous voulez entrer manuellement les adresses 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 iDRAC.

Configuration d'iDRAC avec le schéma étendu d'Active Directory et SM-CLP

REMARQUE : Un serveur TFTP à partir duquel vous pouvez récupérer le certificat d'autorité de certification racine et sur lequel vous pouvez enregistrer le certificat de serveur iDRAC doit s'exécuter.

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory iDRAC avec le schéma étendu via SM-CLP.

1. Ouvrez une session iDRAC via Telnet ou SSH et entrez les commandes SM-CLP suivantes :

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=1

   set oemdell_adracdomain=<FQDN rac>

   set oemdell_adrootdomain=<FQDN racine>

   set oemdell_adracname=<nom de domaine RAC>

   set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD

   load -source <URI TFTP du certificat d'autorité de certification racine>
   ```

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
dump -destination <URI TFTP du certificat de serveur DRAC> /system1/sp1/oemdell_ssl1
```

2. Si DHCP est activé sur iDRAC et que vous voulez utiliser le nom DNS fourni par le serveur DHCP, tapez la commande SM-CLP suivante :

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oemdell_serversfromdhcp=1
```

3. Si DHCP est désactivé sur iDRAC ou que vous voulez entrer manuellement l'adresse IP DNS, tapez les commandes SM-CLP suivantes :

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<adresse IP du serveur DNS principal>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<adresse IP du serveur DNS secondaire>
```

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 iDRAC. Sur Active Directory, un objet de groupe standard est utilisé comme un groupe de rôles. Un utilisateur ayant accès à iDRAC sera membre du groupe de rôles. Pour octroyer à cet utilisateur l'accès à un iDRAC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cet iDRAC. Contrairement à la solution du schéma étendu, le niveau des rôles et des privilèges est défini sur chaque iDRAC et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque iDRAC. Le tableau 5-10 indique les niveaux de privilège des groupes de rôles et le tableau 6-9 indique les paramètres par défaut des groupes de rôles.

Figure 6-4. Configuration d'iDRAC avec Microsoft Active Directory et le schéma standard

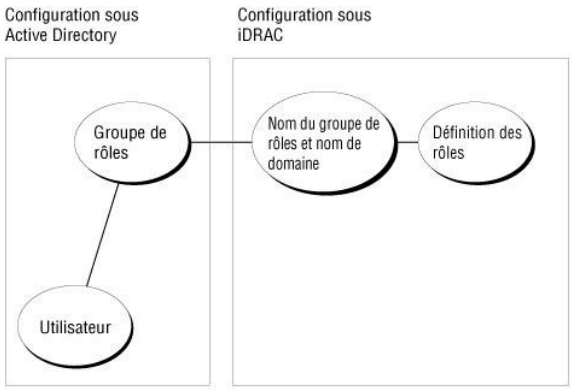


Tableau 6-9. Privilèges par défaut des groupes de rôles

Niveau de privilège par défaut	Droits accordés	Masque binaire
Administrateur	**Ouverture de session** iDRAC, **Configuration d'**iDRAC, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**	0x000001ff
Utilisateur privilégié	**Ouverture de session** iDRAC, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**	0x000000f9
Utilisateur invité	Ouvrir une session iDRAC	0x00000001
Aucun	Aucun droit attribué	0x00000000
Aucun	Aucun droit attribué	0x00000000

REMARQUE : Les valeurs de masque binaire ne sont utilisées que lors du paramétrage du schéma standard avec RACADM.

Il y a deux manières d'activer le schéma standard dans Active Directory :

- Avec l'interface utilisateur Web iDRAC. Voir Configuration d'iDRAC avec le schéma standard d'Active Directory et l'interface Web.
- Avec l'outil CLI RACADM. Voir Configuration d'iDRAC avec le schéma standard d'Active Directory et RACADM.

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

Vous devez effectuer les étapes suivantes pour configurer Active Directory avant qu'un utilisateur Active Directory puisse avoir accès à iDRAC :

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 iDRAC avec l'interface Web, RACADM ou SM-CLP (voir Configuration d'iDRAC avec le schéma standard d'Active Directory et l'interface Web ou Configuration d'iDRAC avec le schéma standard d'Active Directory et RACADM).
3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse accéder à iDRAC.

Configuration d'iDRAC 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 iDRAC.
3. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis sur l'onglet **Configuration**.
4. Sélectionnez **Active Directory** pour ouvrir la page **Menu principal d'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 **privilèges de groupe de rôles** du groupe de rôles.
10. Tapez le **nom du groupe**. Le nom du groupe identifie le groupe de rôles d'Active Directory associé à iDRAC.
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 **Privilèges de groupe de rôles**, définissez les privilèges de groupe.

    Le tableau 5-10 décrit les **privilèges de groupe de rôles**.

    Si vous modifiez des droits, le **privilège du groupe de rôles** actuel (**administrateur**, **utilisateur privilégié** ou **utilisateur invité**) devient celui d'un groupe personnalisé ou un **privilège de groupe de rôles** correspondant aux droits modifiés.
13. Cliquez sur **Appliquer** pour enregistrer les paramètres 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. Téléversez votre certificat d'autorité de certification racine de forêt de domaine dans iDRAC.
    a. Sélectionnez le bouton radio **Téléverser le certificat d'autorité de certification d'Active Directory**, puis cliquez sur **Suivant**.
    b. Sur la page **Téléversement 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 téléversez. 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 accédant à iDRAC (voir Exportation d'un certificat d'autorité de certification racine du contrôleur de domaine).

    c. Cliquez sur **Appliquer**.

    Le serveur Web iDRAC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.

17. Fermez puis ouvrez une session iDRAC pour terminer la configuration de la fonctionnalité Active Directory iDRAC.

18. Cliquez sur **Système**→ **Accès à distance**.

19. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.

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 du schéma standard d'Active Directory iDRAC est terminée.

Configuration d'iDRAC avec le schéma standard d'Active Directory et RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory avec le schéma standard iDRAC via l'interface de ligne de commande 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 <FQDN racine>

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

   racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <FQDN RAC>

   racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <masque binaire des droits>

   racadm sslcertupload -t 0x2 -f <URI TFTP du certificat d'autorité de certification racine>

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

   REMARQUE : Pour des informations sur les valeurs des masques binaires, voir le tableau B-1.

2. Si DHCP est activé sur iDRAC 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 iDRAC ou que vous voulez entrer les adresses IP DNS manuellement, 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>
   ```

Configuration d'iDRAC avec le schéma standard d'Active Directory et SM-CLP

REMARQUE : Vous ne pouvez pas téléverser de certificats via SM-CLP. Utilisez, au contraire, l'interface Web iDRAC ou les commandes RACADM locales.

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory iDRAC avec le schéma standard via SM-CLP.

1. Ouvrez une session iDRAC via Telnet ou SSH et entrez les commandes SM-CLP suivantes :

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=2

   set oemdell_adracdomain=<FQDN RAC>
   ```

2. Entrez les commandes suivantes pour chacun des cinq groupes de rôles Active Directory :

```
set /system1/sp1/groupN nom du groupe_oemdell=<nom de domaine du groupe de rôles N>

set /system1/sp1/groupN domaine du groupe_oemdell=<FQDN rac>

set /system1/sp1/groupN droits du groupe_oemdell=<masque binaire des droits utilisateur>
```

où *N* est un nombre compris entre 1 et 5.

3. Entrez les commandes suivantes pour configurer les certifications SSL Active Directory.

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD
load -source <URI TFTP du certificat d'autorité de certification racine>

set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL

dump -destination <URI TFTP du certificat de serveur iDRAC> /system1/sp1/oemdell_ssl1
```

4. Si DHCP est activé sur iDRAC et que vous voulez utiliser le nom DNS fourni par le serveur DHCP, tapez la commande SM-CLP suivante :

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=1
```

5. Si DHCP est désactivé sur iDRAC ou que vous voulez entrer manuellement les adresses IP DNS, tapez les commandes SM-CLP suivantes :

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<adresse IP du serveur DNS principal>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<adresse IP du serveur 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**→ **Règle de sécurité du 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. Téléversez le certificat que vous avez enregistré à l'étape 14 sur iDRAC.

    Pour téléverser le certificat via RACADM, voir Configuration d'iDRAC avec le schéma étendu d'Active Directory via l'interface Web.

    Pour téléverser le certificat via l'interface Web, effectuez la procédure suivante :

    a. Ouvrez une fenêtre de navigateur Web prise en charge.
    b. Connectez-vous à l'interface Web iDRAC.
    c. Cliquez sur **Système→ Accès à distance**, puis sur l'onglet **Configuration**.
    d. Cliquez sur **Sécurité** pour ouvrir la page **Menu principal du certificat de sécurité**.
    e. Sur la page **Menu principal du certificat de sécurité**, sélectionnez **Téléverser le certificat de serveur** et cliquez sur **Appliquer**.
    f. Sur l'écran **Téléversement d'un certificat**, effectuez l'une des procédures suivantes :
        - Cliquez sur **Parcourir** et sélectionnez le certificat.
        - Dans le champ **Valeur**, tapez le chemin d'accès au certificat.
    g. Cliquez sur **Appliquer**.

Importation du certificat SSL du micrologiciel iDRAC

Utilisez la procédure suivante pour importer le certificat SSL du micrologiciel iDRAC 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 iDRAC est signé par une autorité de certification connue, vous n'avez pas besoin d'effectuer les étapes décrites dans cette section.

Le certificat SSL iDRAC est le même que celui utilisé pour le Web Server iDRAC. Tous les iDRAC sont livrés avec un certificat auto-signé par défaut.

Pour accéder au certificat via l'interface Web iDRAC, sélectionnez **Configuration→ Active Directory→ Télécharger le certificat de serveur iDRAC**.

1. Sur le contrôleur de domaine, ouvrez une fenêtre **Console MMC** et sélectionnez **Certificats→ Autorités de certification racine de confiance**.
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 iDRAC

Vous pouvez utiliser Active Directory pour ouvrir une session iDRAC via l'interface Web. Utilisez l'un des formats suivants pour entrer votre nom d'utilisateur :

<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 6-10 répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 6-10. Utilisation d'iDRAC avec Active Directory : Questions les plus fréquentes

Question	Réponse
Puis-je ouvrir une session iDRAC avec Active Directory sur plusieurs arborescences ?	Oui. L'algorithme de requête Active Directory iDRAC prend en charge plusieurs arborescences d'une seule forêt.
L'ouverture de session iDRAC 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 iDRAC (notamment 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 d'iDRAC 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 car iDRAC ne permet de téléverser qu'un seul certificat SSL d'autorité de certification de confiance.
J'ai créé un nouveau certificat de RAC et je l'ai téléversé ; depuis, l'interface Web ne se lance pas.	Si vous avez utilisé les services de certificats Microsoft pour générer le certificat RAC, vous avez peut-être choisi **Certificat d'utilisateur** au lieu de **Certificat Web** lorsque vous avez créé le certificat. Pour récupérer, générer une RSC, puis créer un nouveau certificat Web à partir des services de certificats Microsoft et le charger via la CLI RACADM du serveur géré, utilisez les commandes RACADM suivantes : racadm sslcsrgen [-g] [-u] [-f {nom de fichier}] racadm sslcertupload -t 1 -f {web_sslcert}
Je n'arrive pas à ouvrir une session iDRAC avec l'authentification d'Active Directory. Qu'est-ce que je peux faire pour résoudre ce problème ?	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 iDRAC local, ouvrez une session iDRAC à l'aide de vos références locales. Une fois la session ouverte, effectuez les étapes suivantes : a. Vérifiez que vous avez coché la case **Activer Active Directory** sur la page **Configuration d'Active Directory** iDRAC. b. Vérifiez que le paramètre DNS est correct sur la page **Configuration réseau** iDRAC. c. Vérifiez que vous avez téléversé le certificat Active Directory sur iDRAC à partir de l'autorité de certification racine 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 iDRAC contient 127 caractères au maximum. Tandis qu'iDRAC peut prendre en charge des mots de passe contenant jusqu'à 256 caractères, Active Directory prend uniquement en charge les mots de passe de 127 caractères au maximum.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de la redirection de console d'interface utilisateur graphique

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Cette section fournit des informations sur l'utilisation de la fonctionnalité de redirection de console iDRAC.

Présentation générale

La fonctionnalité de redirection de console iDRAC 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 iDRAC à partir d'un seul emplacement.

Vous n'avez pas besoin de vous installer devant chaque serveur pour effectuer l'ensemble des opérations de maintenance de routine. Vous pouvez, au contraire, gérer les serveurs depuis n'importe quel endroit, à partir de votre bureau ou ordinateur portable. Vous pouvez aussi partager les informations avec d'autres, à distance et instantanément.

Utilisation de la redirection de console

REMARQUE : Lorsque vous ouvrez une session de redirection de console, le serveur 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 serveur 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 :

- Deux sessions de redirection de console simultanées sont prises en charge au maximum. Les deux sessions affichent la même console de serveur géré simultanément.
- Une session de redirection de console ne doit pas être lancée à partir d'un navigateur Web sur le système géré.
- Une bande de fréquence de réseau disponible minimale de 1 Mo/s est exigée.

Résolutions d'écran prises en charge et fréquences d'actualisation

Le tableau 7-1 répertorie les résolutions d'écran prises en charge et les taux de rafraîchissement correspondants pour une session de redirection de console qui est exécutée sur le serveur 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. Voir les sections suivantes pour plus d'informations :
   - 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.

   - Configuration d'un navigateur Web pris en charge

2. Si vous utilisez Firefox ou souhaitez utiliser le visualiseur Java avec Internet Explorer, installez un environnement d'exécution Java (JRE). Voir Installation d'un environnement d'exécution Java (JRE).

3. Il est recommandé de configurer la résolution d'affichage de votre moniteur sur au moins 1280x1024 pixels.

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

Configuration de la redirection de console dans l'interface Web iDRAC

Pour configurer la redirection de console dans l'interface Web iDRAC, effectuez les étapes suivantes :

1. Cliquez sur **Système**, puis sur l'onglet **Console**.

2. Cliquez sur **Configuration** pour ouvrir la page **Configuration de la redirection de console**.

3. Configurez les propriétés de la redirection de console. Le tableau 7-2 décrit les paramètres de la redirection de console.

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

5. Cliquez sur le bouton approprié pour continuer. Voir tableau 7-3.

Tableau 7-2. Propriétés de configuration de la redirection de console

Propriété	Description
Activé	Cliquez pour activer ou désactiver la redirection de console. **Coché** indique que la redirection de console est activée. **Décoché** indique que la redirection de console est désactivée. **Activé** est sélectionné par défaut.
Nombre maximal de sessions	Affiche le nombre maximal de sessions de redirection de console possibles, **1** ou **2**. Utilisez le menu déroulant pour modifier le nombre maximal de sessions de redirection de console permises. L'adresse par défaut est **2**.
Sessions actives	Affiche le nombre de sessions de consoles actives. Ce champ est en lecture seule.
Numéro de port du clavier et de la souris	Numéro de port réseau utilisé pour connecter à l'option clavier/souris de la redirection de console. Ce trafic est toujours crypté. Vous devrez peut-être changer ce numéro si un autre programme utilise le port par défaut. L'adresse par défaut est **5900**.
Numéro de port vidéo	Le numéro de port réseau utilisé pour connecter le service de l'écran de redirection de console. Vous devrez peut-être modifier ce paramètre si un autre programme utilise le port par défaut. L'adresse par défaut est **5901**.
Cryptage vidéo activé	**Coché** indique que le cryptage vidéo est activé. Tout le trafic allant au port vidéo est crypté. **Décoché** indique que le cryptage vidéo est désactivé. Le trafic allant au port vidéo n'est pas crypté. La valeur par défaut est **Crypté. La désactivation du cryptage peut améliorer les performances sur les réseaux plus lents.**
Mode souris	Sélectionnez **Windows** si le serveur géré fonctionne sous un système d'exploitation Windows. Sélectionnez **Linux** si votre serveur fonctionne sous Linux. Sélectionnez **Aucun** si votre serveur ne fonctionne pas sous un système d'exploitation Windows ou Linux. Le système d'exploitation par défaut est **Windows**.
Type de plug-in de console pour IE	Quand vous utilisez Internet Explorer sur un système d'exploitation Windows, vous pouvez sélectionner l'un des visualiseurs suivants : *ActiveX* : le visualiseur de *redirection* de console ActiveX Java : le visualiseur de redirection de console Java. **REMARQUE :** L'environnement d'exécution Java doit être installé sur votre système client pour pouvoir utiliser le visualiseur Java.
Désactiver la console locale	Si cette case est cochée, cela signifie que la sortie vers le moniteur iKVM est désactivée lors de la redirection de console. Ceci assure que les tâches que vous effectuez avec la **redirection de console** ne sont pas visibles sur le moniteur local du serveur géré.

REMARQUE : Pour plus d'informations sur l'utilisation du média virtuel avec la redirection de console, voir Configuration et utilisation du média virtuel.

Les boutons répertoriés dans le tableau 7-5 sont disponibles sur la page **Configuration de la redirection de console**.

Tableau 7-3. Boutons de la page Configuration de la redirection de console

Bouton	Définition
Imprimer	Imprime la page **Configuration de la redirection de console**.
Actualiser	Recharge la page **Configuration de la redirection de console**
Appliquer	Enregistre les nouveaux paramètres définis sur la redirection de console.

Configuration de la redirection de console dans l'interface de ligne de commande SM-CLP

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 distant à partir de votre station de gestion locale.

Pour ouvrir une session de redirection de console dans l'interface Web, effectuez les étapes suivantes :

1. Cliquez sur **Système**, puis sur l'onglet **Console**.

2. Sur la page **Redirection de console**, utilisez les informations du tableau 7-4 pour vérifier qu'une session de redirection de console est disponible.

   Si vous souhaitez reconfigurer des valeurs de propriété affichées, voir Configuration de la redirection de console dans l'interface Web iDRAC.

Tableau 7-4. Informations de la page Redirection de console

Propriété	Description
Redirection de console activée	Oui/Non
Cryptage vidéo activé	Oui/Non
Nombre maximal de sessions	Affiche le nombre maximal de sessions de redirection de console prises en charge
Sessions ouvertes	Affiche le nombre actuel de sessions de redirection de console ouvertes
Mode souris	Affiche le type d'accélération de la souris actif. Le mode **Accélération de la souris** doit être sélectionné selon le type de système d'exploitation installé sur le serveur géré.
Type de plug-in de console	Indique le type de plug-in configuré. **ActiveX** : un visualiseur Active-X est lancé. Le visualiseur Active-X fonctionne uniquement sur Internet Explorer pendant une exécution sous un système d'exploitation Windows. **Java** : un visualiseur Java est lancé. Le visualiseur Java peut être utilisé sur tous les navigateurs, y compris Internet Explorer. Si votre client ne s'exécute pas sur un système d'exploitation Windows, vous devez alors utiliser le visualiseur Java. Si vous accédez à iDRAC avec Internet Explorer pendant une exécution sous un système d'exploitation Windows, vous pouvez sélectionner Active-X ou Java comme type de plug-in.
Console locale	Cette case est décochée si la console locale n'a pas été désactivée. Si cette case est cochée, la console n'est pas accessible à toute personne utilisant la connexion iKVM sur le châssis.

REMARQUE : Pour plus d'informations sur l'utilisation du média virtuel avec la redirection de console, voir Configuration et utilisation du média virtuel.

Les boutons répertoriés dans le tableau 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**
Lancer le visualiseur	Ouvre une session de redirection de console sur le système distant cible.
Imprimer	Imprime la page **Configuration de la redirection de console**.

3. Si une session de redirection de console est disponible, cliquez sur **Lancer le visualiseur**.

   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 à iDRAC et le bureau du système distant apparaît dans l'application de visualiseur KVM numérique de Dell.

4. Deux pointeurs de souris apparaissent dans la fenêtre du visualiseur : un pour le système distant et l'autre pour votre système local. Vous devez synchroniser les deux pointeurs de souris de sorte que le pointeur de souris distant suive votre pointeur de souris local. Voir Synchronisation des pointeurs de souris.

Utilisation de Video Viewer

L'application Video Viewer fournit une interface utilisateur entre la station de gestion et le serveur géré, vous permettant de visualiser le bureau du serveur géré et de contrôler ses fonctions clavier et souris à partir de votre station de gestion. Lorsque vous vous connectez au système distant, Video Viewer démarre dans une fenêtre séparée.

Video Viewer fournit divers réglages de commandes tels que le mode couleur, la synchronisation de la souris, les instantanés, les macros de clavier et l'accès au média virtuel. 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 devrez peut-être régler le mode couleur et synchroniser les pointeurs de souris.

Le tableau 7-6 décrit les options de menu disponibles dans le visualiseur.

Tableau 7-6. Sélections sur la barre de menus du visualiseur

Élément de menu	Élément	Description
Vidéo	Pause	Interrompt temporairement la redirection de console.
	Reprendre	Reprend la redirection de console.
	Actualiser	Redessine l'image d'écran du visualiseur.
	Capturer l'écran actuel	Capture l'écran du système distant actuel dans un fichier **.bmp** sur Windows ou dans un fichier **.png** sur Linux. Une boîte de dialogue s'affiche pour que vous puissiez enregistrer le fichier dans un emplacement précisé.
	Plein écran	Pour développer le Video Viewer en mode plein écran, sélectionnez **Plein écran** dans le menu **Vidéo**.
	Quitter	Lorsque vous n'avez plus besoin d'utiliser la console et que vous avez fermé la session (en suivant la procédure de fermeture de session du système), sélectionnez **Quitter** dans le menu **Vidéo** pour fermer la fenêtre **Video Viewer**.
Clavier	Touche Alt droite maintenue enfoncée	Sélectionnez cet élément avant de taper sur des touches que vous souhaitez combiner avec la touche <Alt> droite.
	Touche Alt gauche maintenue enfoncée	Sélectionnez cet élément avant de taper sur des touches que vous souhaitez combiner avec la touche <Alt> gauche.
	Touche Windows gauche	Sélectionnez **Maintenir enfoncé** avant de taper des caractères que vous souhaitez combiner avec la touche Windows gauche. Sélectionnez **Appuyer et relâcher** pour envoyer une séquence de touche Windows gauche.
	Touche Windows droite	Sélectionnez **Maintenir enfoncé** avant de taper des caractères que vous souhaitez combiner avec la touche Windows droite. Sélectionnez **Appuyer et relâcher** pour envoyer une séquence de touche Windows droite.
	Macros	Lorsque vous sélectionnez une macro ou son raccourci, l'action s'exécute sur le système distant. Video Viewer fournit les macros suivantes : • Ctrl-Alt-Suppr • Alt-Tab • Alt-Échap • Ctrl-Échap • Alt-Espace • Alt-Entrée • Alt-Tiret • Alt-F4 • ImprÉcran • Alt-ImprÉcran • F1 • Pause • Alt+m
	Transfert des données clavier	Le mode de transfert des données clavier permet à toutes les fonctions clavier du client d'être redirigées vers le serveur.
Souris	Synchroniser le curseur	Le menu **Souris** vous permet de synchroniser le curseur pour que la souris du client soit redirigée vers la souris du serveur.
Options	Mode couleur	Vous permet de sélectionner une profondeur de couleur pour améliorer les performances sur le réseau. Par exemple, si vous installez le logiciel à partir du média virtuel, vous pouvez choisir la profondeur de faible nombre de couleurs (gris 3 bits) de manière à ce que moins de bande passante réseau soit utilisée par le visualiseur de console, laissant ainsi davantage de bande passante pour le transfert des données à partir du média. Le mode couleur peut être défini sur couleur 15 bits, couleur 7 bits, couleur 4 bits, gris 4 bits et gris 3 bits.
Média	Assistant Média virtuel	Le menu **Média** donne accès à l'assistant Média virtuel, qui vous permet de rediriger vers un périphérique ou une image de type : • Lecteur de disquette • CD • DVD • Image au format ISO • Lecteur flash USB Pour plus d'informations sur la fonctionnalité Média virtuel, voir Configuration et utilisation du média virtuel.

		La fenêtre Visualiseur de console doit rester active lorsque vous utilisez le média virtuel.
Aide	-	Active le menu **Aide**.

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 la souris de votre station de gestion, provoquant l'apparition de deux pointeurs de souris dans la fenêtre Video Viewer.

Pour synchroniser les pointeurs de souris, cliquez sur **Souris→ Synchroniser le curseur** ou appuyez sur <Alt><M>.

L'élément de menu Synchroniser le curseur est une touche à bascule. Assurez-vous qu'une coche est insérée en regard de l'élément dans le menu, ce qui permet à la synchronisation de la souris d'être active.

Lorsque vous utilisez Red Hat® Linux® ou Novell® SUSE® Linux, veillez à configurer le mode souris pour Linux avant de lancer le visualiseur. Voir Configuration de la redirection de console dans l'interface Web iDRAC pour obtenir de l'aide concernant la configuration. Les paramètres de souris par défaut du système d'exploitation sont utilisés pour contrôler le curseur de la souris dans l'écran Redirection de console iDRAC.

Désactivation ou activation de la console locale

Vous pouvez configurer iDRAC pour interdire les connexions iKVM via l'interface Web iDRAC. Lorsque la console locale est désactivée, un point de condition jaune apparaît dans la liste des serveurs (OSCAR) pour indiquer que la console est verrouillée dans iDRAC. Lorsque la console locale est activée, le point de condition est vert.

Si vous souhaitez vous assurer que vous disposez d'un accès exclusif à la console de serveur géré, vous devez désactiver la console locale *et reconfigurer le* **nombre maximal de sessions** sur 1 sur la page **Redirection de console**.

REMARQUE : La fonctionnalité de console locale est prise en charge sur tous les systèmes PowerEdge x9xx sauf les systèmes PowerEdge SC1435 et 6950.

REMARQUE : Si vous désactivez (éteignez) la vidéo locale sur le serveur, le moniteur, le clavier et la souris connectés à iKVM sont désactivés.

Pour désactiver ou activer la console locale, effectuez les procédures suivantes :

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session iDRAC. Voir Accès à l'interface Web pour plus d'informations.
2. Cliquez sur **Système**, cliquez sur l'onglet **Console**, puis sur **Configuration**.
3. Si vous voulez désactiver la vidéo locale sur le serveur, sur la page **Configuration de la redirection de console**, cochez la case **Désactiver la console locale**, puis cliquez sur **Appliquer**. La valeur par défaut est **Désactivé**.
4. Si vous voulez activer la vidéo locale sur le serveur, sur la page **Configuration de la redirection de console**, décochez la case **Désactiver la console locale**, puis cliquez sur **Appliquer**.

La page **Redirection de console** affiche la condition de la vidéo du serveur local.

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 lorsque la vidéo locale sur le serveur est désactivée ?	Oui.
Pourquoi la vidéo locale sur le serveur prend-elle 15 secondes pour se désactiver après une requête pour la désactiver ?	Ceci permet à l'utilisateur local d'agir avant que la vidéo ne soit désactivée.
Est-ce qu'il y a un délai quand la vidéo locale est activée ?	Non, une fois que la requête pour **activer** la vidéo locale est reçue par iDRAC, 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 ?	Non. Une fois que la console locale est désactivée, le clavier et la souris de l'utilisateur local sont désactivés et ne sont plus en mesure de modifier des paramètres.
La désactivation de la vidéo locale désactive-t-elle aussi le clavier et la souris locaux ?	Oui.
La désactivation de la console locale	Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de la console distante.

désactive-t-elle la vidéo sur la session de la console distante ?	
Quels sont les privilèges nécessaires à un utilisateur iDRAC pour activer ou désactiver la vidéo du serveur local ?	Tout utilisateur disposant de privilèges de configuration iDRAC peut activer ou désactiver la console locale.
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 iDRAC. La commande CLI RACADM **racadm getconfig –g cfgRacTuning** affiche la condition dans l'objet **cfgRacTuneLocalServerVideo**. La condition est également visible dans l'affichage OSCAR iKVM. Lorsque la console locale est activée, une condition de couleur verte apparaît en regard du nom du serveur. Lorsqu'elle est désactivée, un point jaune indique que la console locale est verrouillée par iDRAC.
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.
La fenêtre de la console est tronquée.	Le visualiseur de console sur Linux requiert un jeu de caractères UTF-8. Vérifiez vos paramètres régionaux et réinitialisez le jeu de caractères si nécessaire. Voir Configuration des paramètres régionaux sous Linux pour plus d'informations.
L'écran du serveur géré est vide lorsque je charge le système d'exploitation Windows 2000. Pourquoi ?	Le serveur géré ne dispose pas du pilote vidéo ATI qui convient. Vous devez mettre à jour le pilote vidéo à l'aide du CD *Dell PowerEdge Installation and Server Management*.
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. De par sa conception, la souris PS/2 utilise la position relative du pointeur de la souris, ce qui entraîne un décalage de synchronisation. iDRAC dispose d'un pilote de souris USB, permettant la position absolue et un suivi plus étroit du pointeur de la souris. Même si iDRAC passait la position absolue de la souris USB au BIOS de Dell, l'émulation du BIOS la reconvertirait en position relative et le comportement ne changerait pas. Pour résoudre ce problème, définissez le mode souris sur **AUCUN** dans la configuration de la redirection de console.
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 la souris appropriée est sélectionnée pour votre système d'exploitation avant de démarrer une session de redirection de console. Assurez-vous que **Synchroniser la souris** est coché dans le menu **Souris**. Appuyez sur <Alt><M> ou sélectionnez **Souris→ Synchroniser la souris** pour faire activer la synchronisation de la souris. Lorsque la synchronisation est activée, une coche apparaît en regard de la sélection dans le menu **Souris**.
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 iDRAC. Pourquoi ?	Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système dont la fonction de redirection de console est activée dans le BIOS, vous recevez un message de connexion EMS qui vous demande de sélectionner **OK** pour pouvoir continuer. Vous ne pouvez pas utiliser la souris pour cliquer sur **OK** à distance. Vous devez sélectionner **OK** sur le système local ou redémarrer le serveur géré à distance, réinstaller puis désactiver la redirection de console dans le BIOS. Ce message est généré par Microsoft pour avertir l'utilisateur que la redirection de console est activée. Pour que ce message n'apparaisse pas, désactivez toujours la redirection de console dans le BIOS avant d'installer un système d'exploitation à distance.
Pourquoi l'indicateur du verrouillage numérique sur ma station de gestion ne reflète-t-il pas la même chose sur le serveur distant ?	Lorsqu'on y accède via iDRAC, 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 Session Viewer apparaissent-elles lorsque j'établis une session de redirection de console à partir de l'hôte local ?	Vous configurez une session de redirection de console à partir du système local. Cette opération n'est pas prise en charge.
Si j'exécute une session de redirection de console et qu'un utilisateur local accède au serveur géré, est-ce que je reçois un message d'avertissement ?	Non. Si un utilisateur local accède au système, vous contrôlez tous deux le système.
Quelle est la bande 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.

Retour à la page du sommaire

Retour à la page du sommaire

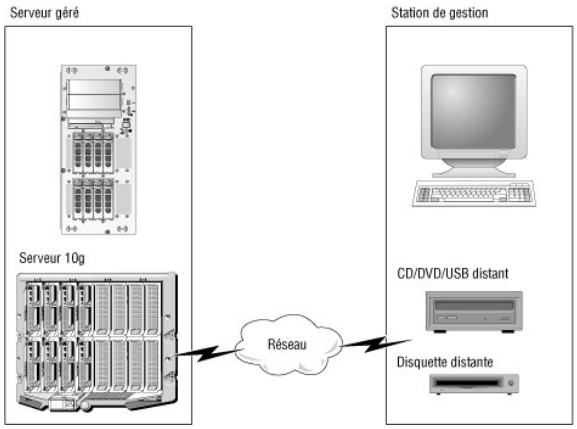
Configuration et utilisation du média virtuel

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Présentation générale

La fonctionnalité **Média virtuel**, accessible via le visualiseur de redirection de console, permet au serveur géré d'accéder au média connecté à un système distant sur le réseau. La figure 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 serveurs gérés, installer des applications, mettre à jour des pilotes ou même installer de nouveaux systèmes d'exploitation à distance à partir de lecteurs de CD/DVD et de disquettes virtuels.

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

Le **média virtuel** définit deux périphériques pour le système d'exploitation et le BIOS du serveur géré : un périphérique de disquette et un périphérique de disque optique.

La station de gestion fournit le média physique ou le fichier image sur le réseau. Lorsque le **média virtuel** est connecté, toutes les requêtes d'accès au lecteur de CD ou de disquette virtuel provenant du serveur géré sont dirigées vers la station de gestion par le réseau. La connexion du **média virtuel** est identique à l'insertion du média dans les périphériques physiques. Lorsque le média virtuel n'est pas connecté, les périphériques virtuels sur le serveur 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/DVD au format ISO9660
Image de lecteur de disquette 1.44	Lecteur de CD-ROM USB avec média CD-ROM.
Disque amovible USB	

Station de gestion Windows

Pour exécuter la fonctionnalité de **média virtuel** sur une station de gestion fonctionnant sous un système d'exploitation Microsoft® Windows®, installez une version prise en charge d'Internet Explorer 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.

Voir Navigateurs Web pris en charge pour plus d'informations.

Vous devez disposer de droits d'administrateur pour installer ActiveX. 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 Firefox. Voir Navigateurs Web pris en charge pour plus d'informations.

Un environnement d'exécution Java (JRE) est requis pour exécuter le plug-in de redirection de console. Vous pouvez télécharger une version JRE à l'adresse **java.sun.com**. La version JRE 1.6 ou supérieure est recommandée.

Configuration du média virtuel

1. Connectez-vous à l'interface Web iDRAC.
2. Sélectionnez **Système** dans l'arborescence et cliquez sur l'onglet **Console**.
3. Cliquez sur **Configuration→ Média virtuel** pour configurer les paramètres du média virtuel.

   Le tableau 8-2 décrit les valeurs de configuration du **média virtuel**.
4. Une fois les paramètres configurés, cliquez sur **Appliquer**.
5. Cliquez sur le bouton approprié pour continuer. Voir tableau 8-3.

Tableau 8-2. Valeurs de configuration du média virtuel

Attribut	Valeur
Connecter le média virtuel	**Connecter** : connecte immédiatement le **média virtuel** au serveur. **Déconnecter** : déconnecte immédiatement le **média virtuel** du serveur. **Autoconnecter** : connecte le **média virtuel** au serveur uniquement quand une session de média virtuel est démarrée.
Nombre maximal de sessions	Affiche le nombre maximal de sessions de **média virtuel** permis. Ce nombre est toujours 1.
Sessions actives	Affiche le nombre actuel de sessions de média virtuel.
Cryptage de média virtuel activé	Cochez la case pour activer ou désactiver le cryptage des connexions du média virtuel. Si cette case est cochée, le cryptage est activé ; si elle est décochée, le cryptage est désactivé.
Numéro de port de média virtuel	Le numéro de port réseau utilisé pour se connecter au service du **média virtuel** sans cryptage. Deux ports consécutifs démarrant à partir du numéro de port spécifié sont utilisés pour la connexion au service du **média virtuel**. Le numéro de port qui suit le port spécifié ne doit pas être configuré pour tout autre service iDRAC. Le numéro de port par défaut est **3668**.
Numéro de port SSL de média virtuel	Le numéro de port réseau utilisé pour les connexions cryptées au service du **média virtuel**. Deux ports consécutifs démarrant à partir du numéro de port spécifié sont utilisés pour la connexion au service du **média virtuel**. Le numéro de port qui suit le port spécifié ne doit pas être configuré pour tout autre service iDRAC. Le numéro de port par défaut est **3670**.
Émulation de disquette	Indique si le **média virtuel** apparaît au serveur comme un lecteur de disquette ou une clé USB. Si l'option **Émulation de disquette** est cochée, le périphérique de **média virtuel** apparaît comme un périphérique de disquette sur le serveur. Si elle est décochée, elle apparaît comme un lecteur de clé USB.
Activer le démarrage une seule fois	Cochez cette case pour activer l'option de démarrage unique. Cette option termine automatiquement la session du **média virtuel** après le premier démarrage du serveur. Cette option est utile pour les déploiements automatisés.

Tableau 8-3. Boutons de la page Configuration du média virtuel

Bouton	Description
Imprimer	Imprime les valeurs de **Configuration de la console** qui apparaissent à l'écran.
Actualiser	Recharge la page **Configuration de la console**.
Appliquer	Enregistre les nouveaux paramètres définis sur la page **Configuration de la console**.

Exécution du média virtuel

AVIS : N'émettez pas une commande **racreset** lorsque vous exécutez une session de **média virtuel**. Sinon, des résultats indésirables peuvent se produire, y compris une perte de données.

AVIS : La fenêtre Visualiseur de console doit rester active lorsque vous accédez au média virtuel.

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion. Voir Navigateurs Web pris en charge.

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

2. Démarrez l'interface Web iDRAC. Accès à l'interface Web.

3. Sélectionnez **Système** dans l'arborescence et cliquez sur l'onglet **Console**.

   La page **Redirection de console** apparaît. Si vous souhaitez modifier les valeurs des attributs affichés, voir Configuration du média virtuel.

   REMARQUE : L'option **Fichier image de disquette** dans **Lecteur de disquette** (si applicable) peut apparaître, comme ce périphérique peut être virtualisé comme un lecteur de disquette virtuel. Vous pouvez sélectionner 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 serveur géré ne coïncident pas avec celles du lecteur physique sur la station de gestion.

   REMARQUE : Le média virtuel peut ne pas fonctionner correctement sur les clients du système d'exploitation Windows qui sont configurés avec l'option de sécurité renforcée d'Internet Explorer. Pour résoudre ce problème, consultez la documentation de votre système d'exploitation Microsoft ou contactez votre administrateur.

4. Cliquez sur **Lancer le visualiseur**.

   REMARQUE : Sous Linux, le fichier **jviewer.jnlp** est téléchargé sur votre bureau et une boîte de dialogue vous demande ce que vous souhaitez faire avec le fichier. Choisissez l'option **Ouvrir avec le programme**, puis sélectionnez l'application **javaws**, qui se trouve dans le sous-répertoire **bin** de votre répertoire d'installation JRE.

   L'application **iDRACView** se lance dans une fenêtre distincte.

5. Cliquez sur **Média→ Assistant Média virtuel...**.

   L'Assistant Redirection de média apparaît.

6. Affichez la fenêtre Condition. Si le média est connecté, vous devez le déconnecter avant d'établir une connexion avec une source de média différente. Cliquez sur le bouton **Déconnecter** situé à droite du média que vous souhaitez déconnecter.

7. Sélectionnez le bouton radio situé en regard des types de média que vous souhaitez connecter.

   Vous pouvez sélectionner un bouton radio dans la section **Lecteur de disquette / USB** et un autre dans la section **Lecteur de CD / DVD**.

   Si vous souhaitez connecter une image de disquette ou une image ISO, entrez le chemin (sur votre ordinateur local) d'accès à l'image ou cliquez sur le bouton **Parcourir** et recherchez l'image.

8. Cliquez sur le bouton **Connecter situé en regard de chaque type de média sélectionné.**

   Le média est connecté et la fenêtre Condition est mise à jour.

9. Cliquez sur le bouton **Fermer.**

Déconnexion du média virtuel

1. Cliquez sur **Média→ Assistant Média virtuel...**.

2. Cliquez sur le bouton **Déconnecter** situé en regard du média que vous souhaitez déconnecter.

   Le média est déconnecté et la fenêtre Condition est mise à jour.

3. Cliquez sur **Fermer**.

Démarrage à partir du média virtuel

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 serveur 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 serveur géré redémarre.

   Le serveur géré essaie de démarrer à partir d'un périphérique d'amorçage en suivant la séquence d'amorçage. Si le périphérique virtuel est connecté et qu'un média de démarrage est présent, le système démarre sur ce périphérique virtuel. Autrement, le système ignore le périphérique, tout comme un périphérique physique sans média de démarrage.

Installation de systèmes d'exploitation 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. Voir Déploiement du système d'exploitation pour plus d'informations.

1. Vérifiez ce qui suit :
   - Le CD d'installation de votre système d'exploitation est inséré dans le lecteur de CD de la station de gestion.
   - Le lecteur de CD local est sélectionné.
   - Vous êtes connecté aux lecteurs virtuels.

2. Suivez les étapes de 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 s'ils sont connectés 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 via l'Assistant Média virtuel, le média est disponible sur le système en cliquant sur le lecteur et en parcourant son contenu.

Systèmes Linux

Selon la configuration du logiciel installé sur votre système, les lecteurs de média virtuel ne peuvent pas être montés automatiquement. Si vos lecteurs ne sont pas montés automatiquement, montez-les manuellement à l'aide de la commande **mount** Linux.

Questions les plus fréquentes

Le tableau 8-4 répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 8-4. Utilisation d'un média virtuel : Questions les plus fréquentes

Question	Réponse
Je remarque parfois que ma connexion de client au Média virtuel est interrompue. Pourquoi ?	Si le délai d'attente du réseau expire, le micrologiciel iDRAC interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. Si les paramètres de configuration du média virtuel sont modifiés dans l'interface Web iDRAC ou via les commandes RACADM locales, tout média connecté est déconnecté lorsque les modifications de la configuration sont appliquées. Pour rétablir la connexion au lecteur virtuel, utilisez l'assistant Média virtuel.

Quels sont les systèmes d'exploitation pris en charge par iDRAC ?	Voir Systèmes d'exploitation pris en charge pour obtenir la liste des systèmes d'exploitation pris en charge.
Quels sont les navigateurs Web pris en charge par iDRAC ?	Voir Navigateurs Web pris en charge pour afficher la liste des navigateurs Web pris en charge.
Pourquoi m'arrive-t-il de perdre parfois ma connexion client ?	• 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. • Si le délai d'attente du réseau expire, le micrologiciel iDRAC interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. En outre, il se peut que quelqu'un ait modifié les paramètres de configuration du média virtuel dans l'interface Web ou en ayant entré des commandes RADACM. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité du **média virtuel**.
Une installation du système d'exploitation Windows semble prendre trop longtemps. Pourquoi ?	Si vous installez le système d'exploitation Windows à l'aide du CD *Dell PowerEdge Installation and Server Management* et en ayant recours à une connexion réseau lente, la procédure d'installation peut nécessiter du temps supplémentaire pour accéder à l'interface Web iDRAC 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 serveur 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 ?	iDRAC vous permet de démarrer à partir des médias de démarrage suivants : • Média de données CD-ROM/DVD • Image ISO 9660 • Disquette 1,44 ou image de disquette • Clé USB qui est reconnue par le système d'exploitation comme disque amovible • Image de clé USB
Comment faire pour pouvoir démarrer à partir de ma clé USB ?	Recherchez l'utilitaire de démarrage Dell sur le site **support.dell.com**, un programme Windows que vous pouvez utiliser pour rendre votre clé USB Dell amorçable. Vous pouvez également démarrer à l'aide d'une disquette d'amorçage Windows 98 et copier les fichiers système de la disquette d'amorçage sur votre clé USB. Par exemple, à l'invite du DOS, tapez la commande suivante : sys a: *x* : /s où *x* : est la clé usb que vous voulez utiliser comme clé de démarrage. Vous pouvez également utiliser l'utilitaire d'amorçage Dell pour créer une 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, naviguez vers le site Web de support de Dell à l'adresse **support.dell.com** et recherchez R122672.exe.
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 attribue au lecteur de disquette virtuel. Procédez comme suit pour rechercher et installer correctement le lecteur de disquette virtuel : 1. Ouvrez une invite de commande Linux et exécutez la commande suivante : grep "Virtual Floppy" /var/log/messages 2. Recherchez la dernière entrée de ce message et notez l'heure. 3. À l'invite de Linux, exécutez la commande suivante : grep "*hh:mm:ss*" /var/log/messages où : *hh:mm:ss* est l'heure du message renvoyé par grep à l'étape 1. 4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique qui est donné à la disquette virtuelle Dell. 5. Assurez-vous que vous êtes relié et connecté au lecteur de disquette virtuel. 6. À l'invite de Linux, exécutez la commande suivante : mount */dev/sdx* /mnt/floppy où : */dev/sdx* est le nom du périphérique trouvé à l'étape 4 /mnt/floppy est le point de montage.
Quels types de systèmes de fichiers sont pris en charge sur mon lecteur de disquette virtuel ?	Votre lecteur de disquette virtuel prend en charge les systèmes de fichiers FAT16 ou FAT32.
Lorsque j'ai effectué une mise à jour de micrologiciel à distance via l'interface Web iDRAC, mes lecteurs virtuels présents sur le serveur ont été supprimés. Pourquoi ?	Les mises à jour de micrologiciel entraînent une réinitialisation d'iDRAC, une interruption de la connexion à distance et le démontage des lecteurs virtuels. Les lecteurs réapparaîtront une fois la réinitialisation d'iDRAC terminée.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de l'interface de ligne de commande RACADM locale

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

L'interface de ligne de commande (CLI) RACADM locale permet d'accéder aux fonctionnalités de gestion iDRAC à partir du serveur géré. RACADM permet d'accéder aux mêmes fonctionnalités que l'interface Web iDRAC. Toutefois, RACADM peut être utilisé dans les scripts afin de faciliter la configuration de plusieurs serveurs et iDRAC, tandis que l'interface Web convient davantage à la gestion interactive.

Les commandes RACADM locales n'utilisent pas les connexions réseau pour accéder à iDRAC à partir du serveur géré. Cela signifie que vous pouvez utiliser les commandes RACADM locales pour configurer la mise en réseau iDRAC initiale.

Pour plus d'informations sur la configuration de plusieurs iDRAC, voir Configuration de plusieurs iDRAC.

Cette section fournit les informations suivantes :

- Utilisation de RACADM à partir d'une invite de commande
- Configuration de votre iDRAC à l'aide de la commande **racadm**
- Utilisation du fichier de configuration RACADM pour configurer plusieurs iDRAC

Utilisation de la commande RACADM

Vous exécutez les commandes RACADM localement (sur le serveur géré) à partir d'une invite de commande ou d'une invite shell.

Connectez-vous au serveur géré, démarrez un environnement de commande et entrez les commandes RACADM locales au format suivant :

```
racadm <sous-commande> -g <groupe> -o <objet> <valeur>
```

Sans options, la commande RACADM affiche des informations d'ordre général. Pour afficher la liste des sous-commandes RACADM, tapez :

```
racadm help
```

La liste des sous-commandes inclut toutes les commandes prises en charge par iDRAC.

Pour obtenir de l'aide concernant une sous-commande, tapez :

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

La commande affiche la syntaxe et les options de ligne de commande de la sous-commande.

Sous-commandes RACADM

Le tableau 9-1 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, voir Présentation de la sous-commande RACADM.

Tableau 9-1. Sous-commandes RACADM

Commande	Description
clrraclog	Efface le journal iDRAC. Une fois cette opération effectuée, une entrée unique est effectuée pour indiquer l'utilisateur et l'heure à laquelle le journal a été effacé.
clrsel	Efface les entrées du journal des événements système du serveur géré.
config	Configure iDRAC.
getconfig	Affiche les propriétés de configuration d'iDRAC actuelles.
getniccfg	Affiche la configuration IP actuelle du contrôleur.
getraclog	Affiche le journal iDRAC.
getractime	Affiche l'heure iDRAC.
getssninfo	Affiche des informations sur les sessions actives.
getsvctag	Affiche les numéros de service.
getsysinfo	Affiche des informations sur iDRAC et le serveur géré, y compris des informations sur la configuration IP, le modèle de matériel, les versions du micrologiciel et sur le système d'exploitation.
gettracelog	Affiche le journal de suivi iDRAC. Si elle est utilisée avec -i, la commande affiche le nombre d'entrées du journal de suivi iDRAC.

help	Répertorie les sous-commandes iDRAC.
help <*sous-commande*>	Répertorie les instructions d'utilisation pour la sous-commande spécifiée.
racreset	Réinitialise iDRAC.
racresetcfg	Restaure la configuration par défaut iDRAC.
serveraction	Effectue des opérations de gestion de l'alimentation sur le serveur géré.
setniccfg	Définit la configuration IP du contrôleur.
sslcertdownload	Télécharge un certificat d'autorité de certification.
sslcertupload	Téléverse un certificat d'autorité de certification ou un certificat de serveur sur iDRAC.
sslcertview	Affiche un certificat d'autorité de certification ou un certificat de serveur iDRAC.
sslcsrgen	Génère et télécharge la RSC SSL.
testemail	Force iDRAC à envoyer un e-mail en passant par le NIC iDRAC.
testtrap	Force iDRAC à envoyer une alerte SNMP en passant par le NIC iDRAC.
vmdisconnect	Force la déconnexion du média virtuel.

Utilisation de l'utilitaire RACADM pour configurer iDRAC

Cette section décrit comment utiliser RACADM pour effectuer diverses tâches de configuration iDRAC.

Affichage des paramètres iDRAC actuels

La sous-commande **getconfig** RACADM récupère les paramètres de configuration actuels à partir d'iDRAC. Les valeurs de configuration sont organisées en *groupes* contenant un ou plusieurs *objets* ayant des *valeurs*.

Voir Définitions des groupes et des objets de la base de données des propriétés iDRAC pour obtenir une description détaillée des groupes et des objets.

Pour afficher la liste de tous les groupes iDRAC, entrez cette commande :

```
racadm getconfig -h
```

Pour afficher les objets et les valeurs d'un groupe spécifique, entrez cette commande :

```
racadm getconfig -g <groupe>
```

Par exemple, pour afficher la liste de tous les paramètres d'objet du groupe **cfgLanNetworking**, tapez la commande suivante :

```
racadm getconfig -g cfgLanNetworking
```

Gestion des utilisateurs iDRAC avec RACADM

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 : Si vous configurez un nouveau iDRAC ou si vous avez exécuté la commande **racadm racresetcfg**, le seul utilisateur actuel est **root** et le mot de passe **calvin**.

REMARQUE : Les utilisateurs peuvent être activés et désactivés à tout moment. Par conséquent, un utilisateur peut avoir un nombre d'index différent sur chaque iDRAC.

Vous pouvez configurer jusqu'à 15 utilisateurs dans la base de données de propriétés iDRAC. (Un seizième utilisateur est réservé pour l'utilisateur LAN IPMI.) Avant d'activer manuellement un utilisateur iDRAC, vérifiez s'il existe des utilisateurs actuels.

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 <*nom de fichier*> et afficher le fichier <*nom de fichier*> généré, qui inclut tous les utilisateurs, ainsi que tous les autres paramètres de configuration iDRAC.

Plusieurs paramètres et numéros d'objets sont affichés avec leurs valeurs actuelles. Les deux objets intéressants sont :

```
# cfgUserAdminIndex=nn

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 signe =, cet index est attribué à ce nom d'utilisateur.

Ajout d'un utilisateur iDRAC

Pour ajouter un nouvel utilisateur à iDRAC, effectuez les étapes suivantes :

1. Définissez le nom d'utilisateur.
2. Définissez le mot de passe.
3. Définissez l'ouverture de session sur les privilèges utilisateur iDRAC.
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 iDRAC :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 jean

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

Pour vérifier le nouvel utilisateur, utilisez l'une des commandes suivantes :

```
racadm getconfig -u jean

racadm getconfig -g cfgUserAdmin -i 2
```

Activation d'un utilisateur iDRAC avec des droits

Pour octroyer à un utilisateur des droits d'administration spécifiques (basés sur les rôles), définissez la propriété **cfgUserAdminPrivilege** sur un masque binaire construit à partir des valeurs affichées dans le tableau 9-2 :

Tableau 9-2. Masques binaires des droits d'utilisateur

Droit d'utilisateur	Masque binaire de privilège
Ouvrir une session iDRAC	0x0000001
Configuration d'iDRAC	0x0000002
Configuration des utilisateurs	0x0000004
Effacer les journaux	0x0000008
Exécution des commandes de contrôle du serveur	0x0000010
Accès à la redirection de console	0x0000020
Accès au média virtuel	0x0000040
Tester les alertes	0x0000080
Exécution des commandes de débogage	0x0000100

Par exemple, pour octroyer à l'utilisateur des privilèges de **configuration d'iDRAC**, de **configuration des utilisateurs**, d'**effacement des journaux** et d'**accès à la redirection de console**, ajoutez les valeurs 0x00000002, 0x00000004, 0x00000008 et 0x00000010 pour construire le bitmap 0x0000002E. Ensuite, entrez la commande suivante pour définir le privilège :

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

Suppression d'un utilisateur iDRAC

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 à iDRAC de supprimer la configuration utilisateur à l'index indiqué et de restaurer les valeurs d'usine par défaut de la configuration utilisateur.

Test des alertes par e-mail

La fonctionnalité des alertes par e-mail iDRAC permet aux utilisateurs de recevoir des alertes par e-mail lorsqu'un événement critique se produit sur le serveur géré. L'exemple suivant montre comment tester la fonctionnalité des alertes par e-mail pour s'assurer qu'iDRAC peut correctement envoyer des alertes par e-mail sur le réseau.

```
racadm testemail -i 2
```

REMARQUE : Assurez-vous que les paramètres des alertes par e-mail sont configurés avant de tester la fonctionnalité d'alertes par e-mail. Voir Configuration des alertes par e-mail pour plus d'informations.

Test de la fonctionnalité d'alertes par interruption SNMP iDRAC

La fonctionnalité d'alertes par interruption SNMP iDRAC permet aux configurations d'écoute d'interruptions SNMP de recevoir des interruptions pour les événements système qui se produisent sur le serveur géré.

L'exemple suivant montre comment un utilisateur peut tester la fonctionnalité d'alertes par interruption SNMP.

```
racadm testtrap -i 2
```

REMARQUE : Avant de tester la fonctionnalité d'alertes par interruption SNMP iDRAC, assurez-vous que les paramètres d'interruption et SNMP sont configurés correctement. Voir les descriptions des sous-commandes **testtrap** et **testemail** pour configurer ces paramètres.

Configuration des propriétés du réseau iDRAC

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'utilitaire de configuration iDRAC lorsque vous êtes invité à taper <Ctrl><E>. Pour plus d'informations sur la configuration des propriétés du réseau à l'aide de l'utilitaire de configuration iDRAC, voir LAN.

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 iDRAC est désactivé même si DHCP est activé.

Configuration d'IPMI

1. Configurez IPMI sur le LAN en entrant la commande suivante :

   ```
   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, voir les spécifications d'IPMI 2.0.

a. Mettez à jour les privilèges de canal IPMI en entrant la commande suivante :

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

où <*niveau*> correspond à :

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

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

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

b. Définissez la clé de cryptage du canal LAN IPMI, si besoin, à l'aide d'une commande similaire à la suivante :

REMARQUE : L'interface IPMI iDRAC prend en charge le protocole RMCP+. Pour plus d'informations, voir les spécifications d'IPMI 2.0.

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

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

2. Configurez les communications série sur le LAN (SOL) IPMI à l'aide de la commande suivante :

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

REMARQUE : 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.

a. Mettez à jour le niveau de privilège minimum SOL IPMI à l'aide de la commande suivante :

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

où <*niveau*> correspond à :

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

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

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

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 serveur géré.

b. Mettez à jour le débit en bauds SOL IPMI à l'aide de la commande suivante :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <débit en bauds>
```

où <*débit en bauds*> est égal à 19200, 57600 ou 115200 b/s.

Par exemple :

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

c. Activez les communications série sur le LAN en tapant la commande suivante à l'invite de commande.

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

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2
```

où <*id*> est l'identifiant unique de l'utilisateur.

Configuration de PEF

Vous pouvez configurer l'action qu'iDRAC devra effectuer pour chaque alerte sur plateforme. Le tableau 9-3 répertorie les actions possibles et la valeur permettant de les identifier dans RACADM.

Tableau 9-3. Action d'événement sur plateforme

Action	Valeur
Pas d'action	0
Mise hors tension	1
Redémarrer	2
Cycle d'alimentation	3

1. Configurez les actions PEF à l'aide de la commande suivante :

   `racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <index> <valeur d'action>`

   où <*index*> est l'index PEF (voir le tableau 5-6, page 62) et <*valeur d'action*> est une valeur du tableau 9-3.

   Par exemple, pour activer PEF pour redémarrer le système et envoyer une alerte IPMI lorsqu'un événement critique de processeur est détecté, tapez la commande suivante :

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
   ```

Configuration de PET

1. Activez les alertes globales à l'aide de la commande suivante :

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

2. Activez PET à l'aide de la commande suivante :

   `racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <index> <0|1>`

   où <*index*> est l'index de destination PET et `0` ou `1` permet, respectivement, de désactiver PET ou d'activer PET.

   Par exemple, pour activer PET avec l'index 4, tapez la commande suivante :

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

3. Configurez votre règle PET à l'aide de la commande suivante :

   `racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <index> <adresse IP>`

   où <*index*> est l'index de destination PET et <*adresse IP*> l'adresse IP de destination du système qui reçoit les alertes d'événement sur plateforme.

4. Configurez la chaîne de nom de communauté.

   À l'invite de commande, tapez :

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

   où <*nom*> est le nom de communauté PET.

Configuration des alertes par e-mail

1. Activez les alertes globales en entrant la commande suivante :

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

2. Activez les alertes par e-mail en entrant les commandes suivantes :

   `racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <index> <0|1>`

   où <*index*> est l'index de destination d'e-mail et 0 désactive l'alerte par e-mail ou 1 active l'alerte. L'index de destination d'e-mail peut être une valeur de 1 à 4.

   Par exemple, pour activer l'e-mail avec l'index 4, tapez la commande suivante :

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Configurez vos paramètres de messagerie en entrant la commande suivante :

   `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.

4. Pour configurer un message personnalisé, entrez la commande suivante :

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <index> <message personnalisé>
   ```

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

5. Testez l'alerte par e-mail configurée, si vous le souhaitez, en entrant la commande suivante :

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

   où <*index*> est l'index de destination d'e-mail à tester.

Configuration du filtrage IP (IpRange)

Le filtrage des adresses IP (ou *contrôle de plage IP*) permet uniquement un accès à iDRAC à partir des clients ou stations de gestion dont les adresses IP sont comprises dans une plage spécifique à l'utilisateur. Toutes les autres requêtes d'ouverture de session sont rejetées.

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** :

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propriété **cfgRacTuneIpRangeMask** est appliquée à l'adresse IP entrante et aux propriétés **cfgRacTuneIpRangeAddr**. Si les résultats sont identiques, la requête d'ouverture de session entrante est autorisée pour pouvoir accéder à iDRAC. Les ouvertures de session à partir d'adresses IP situées à l'extérieur de cette plage reçoivent un message d'erreur.

L'ouverture de session a lieu si l'expression suivante est égale à zéro :

```
cfgRacTuneIpRangeMask & (<adresse IP entrante> ^ cfgRacTuneIpRangeAddr)
```

où & est l'opérateur bitwise AND des quantités et ^ est l'opérateur bitwise exclusif OR.

Voir cfgRacTuning pour afficher la liste complète des propriétés **cfgRacTuning**.

Tableau 9-4. Propriétés de filtrage des adresses IP (IpRange)

Propriété	Description
cfgRacTuneIpRangeEnable	Active la fonctionnalité de contrôle de plage IP.
cfgRacTuneIpRangeAddr	Détermine le format binaire d'adresse IP autorisé, en fonction des 1 dans le masque de sous-réseau. Cette propriété correspond à l'opérateur *AND* avec **cfgRacTuneIpRangeMask** pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP contenant cette configuration binaire dans ses bits de niveau supérieur est autorisée à ouvrir une session. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échouent. Les valeurs par défaut de chaque propriété autorisent une plage d'adresse allant de 192.168.1.0 à 192.168.1.255 pour ouvrir une session.
cfgRacTuneIpRangeMask	Définit les positions de bit significatives dans l'adresse IP. Le masque doit avoir la forme d'un masque de réseau, où les bits les plus significatifs sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur.

Configuration du filtrage IP

Pour configurer le filtrage IP dans l'interface Web, suivez ces étapes :

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**.
2. Sur la page **Configuration réseau**, cliquez sur **Paramètres avancés**.
3. Cochez la case **Plage IP activée** et entrez l'**adresse de la plage IP** et le **masque de sous-réseau de la plage IP**.
4. Cliquez sur **Appliquer**.

Les exemples suivants utilisent la commande RACADM locale pour configurer le filtrage IP.

REMARQUE : Voir Utilisation de l'interface de ligne de commande RACADM locale pour plus d'informations sur RACADM et les commandes RACADM.

1. Les commandes RACADM suivantes bloquent toutes les adresses IP sauf 192.168.0.57 :

   ```
   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
```

2. 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
```

Le dernier octet du masque de plage est défini sur 252, l'équivalent décimal de 11111100b.

Consignes concernant le filtrage IP

Observez les consignes suivantes lorsque vous activez le filtrage IP :

- Assurez-vous que **cfgRacTuneIpRangeMask** est configuré sous forme de masque de réseau, où les bits les plus significatifs sont des 1 (ce qui définit le sous-réseau dans le masque) avec une transition de tous les 0 dans les bits les moins significatifs.
- 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.

Configuration du blocage IP

Le blocage IP détermine de manière dynamique à quel moment un nombre excessif d'échecs d'ouverture de session se produit à partir d'une adresse IP particulière et empêche l'adresse de se connecter à iDRAC pendant une période prédéfinie.

Les fonctionnalités de blocage IP incluent :

- Le nombre d'échecs d'ouverture de session autorisés (**cfgRacTuneIpBlkFailcount**)
- Le laps de temps, en secondes, au cours duquel ces échecs doivent se produire (**cfgRacTuneIpBlkFailWindow**)
- La durée, en secondes, pendant laquelle l'adresse IP bloquée ne peut établir une session lorsque le nombre d'échecs autorisés est dépassé (**cfgRacTuneIpBlkPenaltyTime**)

Étant donné que 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.

Voir Définitions des groupes et d'objets de la base de données des propriétés iDRAC pour obtenir une liste complète des propriétés **cfgRacTune**.

Les propriétés de restriction des nouvelles tentatives d'ouverture de session répertorient les paramètres définis par l'utilisateur.

Tableau 9-5. 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	Le laps de temps, en secondes, au cours duquel les tentatives ayant échoué sont comptées. Lorsque le nombre d'échecs dépasse cette limite, le compteur est remis à zéro.
cfgRacTuneIpBlkPenaltyTime	Définit la 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.

Activation du blocage IP

L'exemple suivant empêche une adresse IP client d'ouvrir une session pendant cinq minutes si ce client a échoué au cours de 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 cfgRacTuneIpBlkFailWindow 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 cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

Configuration de services Telnet et SSH iDRAC via RACADM local

La console Telnet/SSH peut être configurée localement (sur le serveur géré) à l'aide des commandes RACADM.

REMARQUE : Vous devez disposer du droit de **configuration d'iDRAC** pour exécuter les commandes dans cette section.

REMARQUE : Lorsque vous reconfigurez les paramètres Telnet ou SSH dans iDRAC, toutes les sessions ouvertes prennent fin sans avertissement.

Pour activer Telnet et SSH depuis la commande RACADM locale, connectez-vous au serveur géré et tapez les commandes suivantes à l'invite de commande :

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

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

Pour désactiver le service Telnet ou SSH, modifiez la valeur `1` pour la définir sur `0` :

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

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

Tapez la commande suivante pour changer le numéro du port Telnet iDRAC :

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

Par exemple, pour modifier le port Telnet 22 par défaut et le définir sur 8022, tapez cette commande :

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Pour afficher la liste complète des commandes CLI RACADM disponibles, voir Utilisation de l'interface de ligne de commande RACADM locale.

Utilisation d'un fichier de configuration iDRAC

Un fichier de configuration iDRAC est un fichier texte contenant une représentation des valeurs dans la base de données iDRAC. Vous pouvez utiliser la sous-commande **getconfig** RACADM pour générer un fichier de configuration contenant les valeurs actuelles d'iDRAC. Vous pouvez ensuite modifier le fichier et utiliser la sous-commande **config -f** RACADM pour recharger le fichier dans iDRAC ou pour copier la configuration sur d'autres iDRAC.

Création d'un fichier de configuration iDRAC

Le fichier de configuration est un fichier texte ordinaire (non formaté). Vous pouvez utiliser n'importe quel nom de fichier valide ; l'extension de fichier **.cfg** est une convention recommandée.

Le fichier de configuration peut être :

- Créé à l'aide d'un éditeur de texte
- Obtenu auprès d'iDRAC avec la sous-commande **getconfig** RACADM
- Obtenu auprès d'iDRAC avec la sous-commande **getconfig** RACADM, puis modifié

Pour obtenir un fichier de configuration, avec la commande **getconfig** RACADM, entrez la commande suivante à l'invite de commande sur le serveur géré :

```
racadm getconfig -f myconfig.cfg
```

Cette commande crée le fichier **myconfig.cfg** dans le répertoire actuel.

Syntaxe du fichier de configuration

AVIS : Modifiez le fichier de configuration à l'aide d'un éditeur de texte ordinaire, tel que le **Bloc-notes** sous Windows ou **vi** sous Linux. L'utilitaire **racadm** analyse le texte ASCII uniquement. Tout formatage peut troubler l'analyseur et corrompre ainsi la base de données iDRAC.

Cette section décrit le format du fichier de configuration.

- Les lignes qui commencent par # sont des commentaires.

  Un commentaire *doit* démarrer dans la première colonne de la ligne. Un caractère # dans toute autre colonne est traité comme un caractère # normal.

  Exemple :

  ```
  #

  # This is a comment

  [cfgUserAdmin]

  cfgUserAdminPrivilege=4
  ```

- Les entrées de groupe doivent être entourées 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 des propriétés iDRAC.

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

  Par exemple :

  `[cfgLanNetworking]` (*nom du groupe*)

  `cfgNicIpAddress=143.154.133.121` (*nom de l'objet*)

- Les paramètres sont spécifiés en tant que paires *objet*=*valeur* sans espace entre l'objet, le signe = et la valeur.

  Tout espace blanc inclus après la valeur est ignoré. L'espace blanc à l'intérieur d'une chaîne de caractères de valeur n'est pas modifié. Tout caractère à droite du signe = est pris tel quel (par exemple, un deuxième signe = ou un #, *[*, *]*, et ainsi de suite).

- L'analyseur ignore une entrée d'objet d'index.

  Vous *ne pouvez pas* spécifier l'index utilisé. 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>` place un commentaire devant les objets d'index, ce qui vous permet de visualiser les commentaires inclus.

REMARQUE : Vous pouvez créer un groupe indexé manuellement à l'aide de la commande suivante :
`racadm config -g <nom du groupe> -o <objet ancré> -i <index> <nom d'ancre unique>`

- La ligne d'un groupe indexé *ne peut pas* être supprimée d'un fichier de configuration.

  Vous devez supprimer un objet indexé manuellement à l'aide de la commande suivante :

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

REMARQUE : Une chaîne de caractères nulle (identifiée par deux caractères "") ordonne à iDRAC de supprimer l'index du groupe spécifié.

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

  ```
  racadm getconfig -g <nom du groupe> -i <index>
  ```

- 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 d'utilisateur>
  ```

- Si l'analyseur rencontre un groupe indexé, c'est la valeur de l'objet ancré qui différencie les différents index.

  L'analyseur lit tous les index du contrôleur iDRAC pour ce groupe-là. Les objets présents dans ce groupe sont de simples modifications lorsque iDRAC est configuré. Si un objet modifié représente un nouvel index, l'index est créé sur iDRAC au cours de la configuration.

- Vous ne pouvez pas spécifier d'index désiré dans un fichier de configuration.

  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 offre une certaine flexibilité lors de l'ajout d'entrées indexées où vous n'avez pas besoin de faire des correspondances d'index exactes entre tous les RAC gérés. De nouveaux utilisateurs sont ajoutés au premier index disponible. Un fichier de configuration qui analyse et s'exécute correctement sur un iDRAC peut ne pas s'exécuter correctement sur un autre si tous les index sont remplis et qu'un nouvel utilisateur doit être ajouté.

Modification de l'adresse IP iDRAC dans un fichier de configuration

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

Par exemple :

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Le fichier sera mis à jour de la manière suivante :

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

cfgNicGateway=10.35.9.1
```

Chargement du fichier de configuration dans iDRAC

La commande `racadm config -f <nom de fichier>` analyse le fichier de configuration afin de s'assurer que des noms d'objet et de groupe valides sont présents et que les règles de syntaxe sont respectées. Si le fichier est exempt d'erreur, la commande met alors à jour la base de données iDRAC avec le contenu du fichier.

REMARQUE : Pour vérifier la syntaxe uniquement et ne pas mettre à jour la base de données iDRAC, ajoutez l'option **-c** à la sous-commande **config**.

Les erreurs détectées dans le fichier de configuration sont indiquées avec le numéro de ligne et un message qui explique le problème. Vous devez corriger toutes les erreurs pour que le fichier de configuration puisse mettre à jour iDRAC.

AVIS : Utilisez la sous-commande **racresetcfg** pour rétablir les paramètres par défaut de la base de données et du NIC iDRAC 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.

Avant d'exécuter la commande `racadm config -f <nom de fichier>`, vous pouvez exécuter la sous-commande **racreset** pour rétablir les paramètres par défaut d'iDRAC. Assurez-vous que le fichier de configuration que vous allez charger inclut tous les objets, utilisateurs, index et autres paramètres souhaités.

Pour mettre à jour iDRAC avec le fichier de configuration, exécutez la commande suivante à l'invite de commande du serveur géré :

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

Lorsque la commande s'est exécutée, vous pouvez exécuter la sous-commande **getconfig** RACADM pour confirmer que la mise à jour a réussi.

Configuration de plusieurs iDRAC

À l'aide d'un fichier de configuration, vous pouvez configurer d'autres iDRAC avec des propriétés identiques. Suivez ces étapes pour configurer plusieurs iDRAC :

1. Créez le fichier de configuration de l'iDRAC dont vous souhaitez répliquer les paramètres vers les autres iDRAC. À l'invite de commande sur le serveur géré, entrez la commande suivante :

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

   où *<nom de fichier>* est le nom du fichier dans lequel sont enregistrées les propriétés iDRAC, comme par exemple **myconfig.cfg**.

   Voir Création d'un fichier de configuration iDRAC pour plus d'informations.

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

2. Modifiez le fichier de configuration que vous avez créé à l'étape précédente et supprimez ou commentez les paramètres que vous *ne voulez pas* répliquer.

3. Copiez le fichier de configuration modifié sur un lecteur réseau où il est accessible à chaque serveur géré pour lequel vous souhaitez configurer iDRAC.

4. Pour chaque iDRAC que vous souhaitez configurer :

   a. Connectez-vous au serveur géré et démarrez une invite de commande.

   b. Si vous souhaitez reconfigurer iDRAC à partir des paramètres par défaut, entrez la commande suivante :

      ```
      racadm racreset
      ```

   c. Chargez le fichier de configuration dans iDRAC à l'aide de la commande suivante :

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

      où <*nom de fichier*> est le nom du fichier de configuration que vous avez créé. Incluez le chemin complet si le fichier ne se trouve pas dans le répertoire de travail.

   d. Réinitialisez l'iDRAC configuré en entrant la commande suivante :

      ```
      racadm reset
      ```

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de l'interface de ligne de commande SM-CLP iDRAC

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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 à iDRAC.

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, voir le site Web de DMTF (Distributed Management Task Force) à l'adresse suivante : **www.dmtf.org**.

SM-CLP iDRAC 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.

L'interface SM-CLP intègre un sous-ensemble des fonctionnalités fournies par l'interface de ligne de commande RACADM locale, mais avec un chemin d'accès différent. L'interface SM-CLP s'exécute au sein d'iDRAC, tandis que RACADM s'exécute sur le serveur géré. En outre, RACADM est une interface propriétaire Dell, tandis que SM-CLP est une interface standard du secteur. Voir Équivalences RACADM et SM-CLP pour obtenir un adressage des commandes RACADM et SM-CLP.

System Management avec SM-CLP

L'interface SM-CLP iDRAC vous permet de gérer les fonctionnalités système suivantes à partir d'une ligne de commande ou d'un script :

- Gestion de l'alimentation du serveur : allume, arrête ou redémarre le système
- Gestion du journal des événements système (SEL) : affiche ou efface les enregistrements SEL
- Gestion de compte utilisateur iDRAC
- Configuration d'Active Directory
- Configuration du LAN iDRAC
- Génération de la requête de signature de certificat (RSC) SSL
- Configuration du média virtuel
- Redirection des communications série sur le LAN (SOL) via Telnet ou SSH

Prise en charge de SM-CLP iDRAC

L'interface SM-CLP est hébergée par le micrologiciel iDRAC et prend en charge les connexions Telnet et SSH. L'interface SM-CLP iDRAC 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 iDRAC.

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.

SM-CLP encourage la conception de verbes et de cibles pour fournir des capacités de configuration 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.

La syntaxe suivante s'applique à la ligne de commande SM-CLP :

```
<verbe> [<options>] [<cible>] [<propriétés>]
```

Le tableau 10-1 fournit une liste des verbes pris en charge par l'interface de ligne de commande iDRAC, la syntaxe de chaque commande et une liste des options prises en charge par le verbe.

Tableau 10-1. Verbes de l'interface de ligne de commande SM-CLP pris en charge

Verbe	Description	Options

cd	Navigue dans l'espace d'adressage du système géré via l'environnement. Syntaxe : cd [*options*] [*cible*]	–default, –examine, –help, –output, –version
delete	Supprime une instance d'objet. Syntaxe : delete [*options*] *cible*	–examine, –help, –output, –version
dump	Déplace une image binaire de MAP vers un URI. dump -destination <*URI*> [*options*] [*cible*]	–destination, –examine, –help, –output, –version
exit	Quitte la session d'environnement SM-CLP. Syntaxe : exit [*options*]	–help, –output, –version
help	Affiche l'aide pour les commandes SM-CLP. help	-examine, -help, -output, -version
load	Déplace une image binaire d'un URI vers MAP. Syntaxe : load -source <*URI*> [*options*] [*cible*]	–examine, –help, –output, –source, –version
reset	Réinitialise la cible. Syntaxe : reset [*options*] [*cible*]	–examine, –help, –output, –version
set	Définit les propriétés d'une cible Syntaxe : set [*options*] [*cible*] <*nom de propriété*>=<*valeur*>	–examine, –help, –output, –version
show	Affiche les propriétés cibles, les verbes et les sous-cibles. Syntaxe : show [*options*] [*cible*] <*nom de propriété*>=<*valeur*>	-all, -default, –display, –examine, –help, –level, –output, –version
start	Démarre une cible. Syntaxe : start [*options*] [*cible*]	–examine, –force, –help, –output, –version
stop	Désactive une cible. Syntaxe : stop [*options*] [*cible*]	–examine, –force, –help, –output, –state, –version, –wait
version	Affiche les attributs de version d'une cible. Syntaxe : version [*options*]	–examine, –help, –output, –version

Le tableau 10-2 décrit les options SM-CLP. Certaines options ont des formes abrégées, comme indiqué dans le tableau.

Tableau 10-2. Options SM-CLP prises en charge

Option SM-CLP	Description
–all, –a	Donne l'ordre au verbe d'effectuer toutes les fonctionnalités possibles.
-destination	Spécifie l'emplacement de stockage d'une image dans la commande dump. Syntaxe : -destination <URI>
-display, -d	Filtre le résultat de la commande. Syntaxe : -display <propriétés | cibles | verbes>[, <propriétés | cibles | verbes>]*
-examine, -x	Donne l'ordre au processeur de commandes de valider la syntaxe de commande sans exécuter la commande.

–help, –h	Affiche l'aide pour le verbe.
–level, -l	Donne l'ordre au verbe d'agir sur les cibles à des niveaux supplémentaires sous la cible spécifiée. Syntaxe : `-level <n | all>`
–output, –o	Spécifie le format de la sortie. Syntaxe : `-output <texte | clpcsv | clpxml>`
-source	Spécifie l'emplacement d'une image dans une commande load. Syntaxe : -source <URI>
–version, –v	Affiche le numéro de version SMASH-CLP.

Navigation dans l'espace d'adressage MAP

REMARQUE : La barre oblique (/) et la barre oblique inverse (\) sont interchangeables dans les chemins d'adresse SM-CLP. Toutefois, une barre oblique inverse située à la fin d'une ligne de commande permet de continuer la commande à la ligne suivante et est ignorée lorsque la commande est analysée.

Les objets pouvant être gérés via SM-CLP sont représentés par des cibles disposées dans un espace hiérarchique appelé espace d'adressage MAP (Manageability Access Point). Un chemin d'adresse spécifie le chemin de la racine de l'espace d'adressage vers un objet dans l'espace d'adressage.

La cible racine est représentée par une barre oblique (/) ou une barre oblique inverse (\). Il s'agit du point de démarrage par défaut lorsque vous ouvrez une session iDRAC. Naviguez à partir de la racine à l'aide du verbe cd. Par exemple, pour naviguer vers le troisième enregistrement du journal des événements système (SEL), entrez la commande suivante :

```
->cd /system1/sp1/logs1/record3
```

Entrez le verbe cd sans cible pour trouver votre emplacement actuel dans l'espace d'adressage. Les abréviations . . et . fonctionnent de la même manière que sous Windows et Linux : . . se réfère au niveau parent et . se réfère au niveau actuel.

Cibles

Le tableau 10-3 fournit une liste des cibles disponibles dans l'interface SM-CLP.

Tableau 10-3. Cibles SM-CLP

Cible	Définition
/system1/	Cible du système géré.
/system1/sp1	Processeur du service.
/system1/sol1	Cible des communications série sur le LAN.
/system1/sp1/account1 through /system1/sp1/account16	Seizième compte utilisateur iDRAC local. account1 est le compte racine.
/system1/sp1/enetport1	Adresse MAC du NIC iDRAC.
/system1/sp1/enetport1/lanendpt1/ ipendpt1	Paramètres IP, de passerelle et de masque réseau iDRAC.
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	Paramètres du serveur DNS iDRAC.
/system1/sp1/group1 through /system1/sp1/group5	Groupes de schéma standard d'Active Directory.
/system1/sp1/logs1	Cible des collections de journal.
/system1/sp1/logs1/record1	Instance d'enregistrement SEL individuelle sur le système géré.
/system1/sp1/logs1/records	Cible du journal SEL sur le système géré.
/system1/sp1/oemdell_racsecurity1	Stockage des paramètres utilisés pour générer une requête de signature de certificat.
/system1/sp1/oemdell_ssl1	État de la requête de certificat SSL.
/system1/sp1/oemdell_vmservice1	Configuration et état du média virtuel.

Utilisation du verbe Show

Pour en savoir plus sur une cible, utilisez le verbe show. Ce verbe affiche les propriétés de la cible, les sous-cibles et une liste des verbes SM-CLP autorisés à cet emplacement.

Utilisation de l'option -display

L'option **show –display** vous permet de restreindre la sortie de la commande à un(e) ou plusieurs propriétés, cibles et verbes. Par exemple, pour afficher uniquement les propriétés et cibles à l'emplacement actuel, utilisez la commande suivante :

```
show -d properties,targets /system1/sp1/account1
```

Pour répertorier uniquement certaines propriétés, qualifiez-les, comme dans la commande suivante :

```
show -d properties=(userid,username) /system1/sp1/account1
```

Si vous souhaitez uniquement afficher une propriété, vous pouvez omettre les parenthèses.

Utilisation de l'option -level

L'option **show -level** exécute le verbe **show** sur les niveaux supplémentaires sous la cible spécifiée. Par exemple, si vous souhaitez afficher les propriétés **nom d'utilisateur** et **id utilisateur** des cibles **account1** à **account16** sous **/system1/sp1**, entrez la commande suivante :

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

Pour afficher toutes les cibles et propriétés de l'espace d'adressage, utilisez l'option **-l all**, comme dans la commande suivante :

```
show -l all -d properties /
```

Utilisation de l'option -output

L'option **-output** spécifie l'un des quatre formats de sortie suivants pour les verbes SM-CLP : **texte**, **clpcsv**, **mot clé** et **clpxml**.

Le format **texte** est le format par défaut ; il s'agit de la sortie la plus lisible. Le format **clpcsv** est un format de valeurs séparées par une virgule approprié au chargement dans un tableur. Le format **mot clé** sort des informations sous forme de liste de paires mot clé=valeur, une par ligne. Le format **clpxml** est un document XML contenant un élément XML de **réponse**. DMTF a spécifié les formats **clpcsv** et **clpxml**, et leurs spécifications sont disponibles sur le site Web DMTF à l'adresse **www.dmtf.org**.

L'exemple suivant montre comment faire apparaître le contenu du journal SEL au format XML :

```
show -l all -output format=clpxml /system1/sp1/logs1
```

Exemples de SM-CLP iDRAC

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

- Gestion de l'alimentation du serveur
- Gestion SEL
- Navigation de la cible MAP
- Affichage des propriétés du système
- Configuration de l'adresse IP, du masque de sous-réseau et de l'adresse de passerelle iDRAC

Gestion de l'alimentation du serveur

Le tableau 10-4 fournit des exemples d'utilisation de SM-CLP pour effectuer des opérations de gestion de l'alimentation sur un serveur géré.

Tableau 10-4. Opérations de gestion de l'alimentation du serveur

Opération	Syntaxe
Connexion à iDRAC via l'interface SSH	>SSH 192.168.0.120 >login: root >password:
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 10-5 fournit des exemples d'utilisation de SM-CLP pour effectuer des opérations SEL sur le système géré.

Tableau 10-5. Opérations de gestion SEL

Opération	Syntaxe
Affichage du journal SEL	->show /system1/sp1/logs1 Targets: record1 record2 record3 record4 record5 Properties : Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs: cd delete exit help show version
Affichage de l'enregistrement SEL	->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4 Properties : Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007 Verbs: cd exit help show version
Effacement du journal SEL	->delete /system1/sp1/logs1 All records deleted successfully

Navigation de la cible MAP

Le tableau 10-6 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 10-6. Opérations de navigation de cible MAP

Opération	Syntaxe
Naviguer vers la cible système et redémarrer	->cd system1 ->reset **REMARQUE :** La cible par défaut actuelle est /.
Naviguer vers la cible SEL et afficher les enregistrements du journal	->cd system1 ->cd sp1 ->cd logs1 ->show
	->cd system1/sp1/logs1 ->show
Afficher la cible actuelle	->cd .
Monter d'un niveau	->cd ..
Quitter l'environnement	->exit

Configuration de l'adresse IP, du masque de sous-réseau et de l'adresse de passerelle iDRAC

L'utilisation de SM-CLP pour mettre à jour les propriétés du réseau iDRAC s'articule autour d'un processus en deux parties :

1. Définissez de nouvelles valeurs pour les propriétés du NIC à l'emplacement **/system1/sp1/enetport1/lanendpt1/ipendpt1:**
   - **oemdell_nicenable** : définie sur 1 pour activer la mise en réseau iDRAC, sur 0 pour la désactiver
   - **ipaddress** : l'adresse IP
   - **subnetmask** : le masque de sous-réseau
   - **oemdell_usedhcp** : définie sur 1 pour activer l'utilisation de DHCP pour définir les propriétés **ipaddress** et **subnetmask**, sur 0 pour définir les valeurs statiques
2. Validez les nouvelles valeurs en définissant la propriété **committed** sur 1.

Lorsque la propriété **commit** a la valeur 1, les paramètres actuels des propriétés sont actifs. Lorsque vous modifiez l'un des paramètres, la propriété **commit** est redéfinie sur 0 pour indiquer que les valeurs n'ont pas été validées.

REMARQUE : La propriété **commit** affecte uniquement les propriétés qui se trouvent à l'emplacement MAP **/system1/sp1/enetport1/lanendpt1/ipendpt1**. Toutes les autres commandes SM-CLP prennent effet immédiatement.

REMARQUE : Si vous utilisez la commande RACADM locale pour définir les propriétés du réseau iDRAC, vos modifications prennent effet immédiatement car la commande RACADM locale ne dépend pas d'une connexion réseau.

Lorsque vous validez les modifications, les nouveaux paramètres réseau prennent effet, ce qui entraîne l'interruption de votre session Telnet ou SSH. En introduisant l'étape de validation, vous pouvez retarder la fermeture de votre session jusqu'à ce que vous ayez exécuté l'ensemble de vos commandes SM-CLP.

Le tableau 10-7 fournit des exemples de configuration des propriétés iDRAC via SM-CLP.

Tableau 10-7. Configuration des propriétés de mise en réseau iDRAC avec SM-CLP

Opération	Syntaxe
Accéder à l'emplacement des propriétés du NIC iDRAC	`->cd /system1/sp1/enetport1/lanendpt1/ipendpt1`
Définir la nouvelle adresse IP	`->set ipaddress=10.10.10.10`
Définir le masque de sous-réseau	`->set subnetmask=255.255.255.255`
Activer l'indicateur DHCP	`->set oemdell_usedhcp=1`
Activer le NIC	`->set oemdell_nicenable=1`
Valider les modifications	`->set committed=1`

Mise à jour du micrologiciel iDRAC via SM-CLP

Pour mettre à jour le micrologiciel iDRAC à l'aide de SM-CLP, vous devez connaître l'URI TFTP du progiciel de mise à jour Dell.

Suivez ces étapes pour mettre à jour le micrologiciel à l'aide de la commande SM-CLP :

1. Ouvrez une session iDRAC via Telnet ou SSH.
2. Vérifiez la version actuelle du micrologiciel en entrant la commande suivante :

   ```
   version
   ```

3. Entrez la commande suivante :

   ```
   load -source tftp://<serveur tftp>/<chemin de mise à jour> /system1/sp1
   ```

   où <*serveur tftp*> est le nom DNS ou l'adresse IP de votre serveur TFTP et <*chemin de mise à jour*> est le chemin d'accès au progiciel de mise à jour sur le serveur TFTP.

   Votre session Telnet ou SSH sera terminée. Vous devrez peut-être patienter plusieurs minutes afin que la mise à jour de micrologiciel puisse se terminer.

4. Pour vérifier que le nouveau micrologiciel a été écrit, démarrez une nouvelle session Telnet ou SSH et entrez de nouveau la commande version.

Utilisation des communications série sur le LAN (SOL) avec Telnet ou SSH

Utilisez une console Telnet ou SSH sur votre station de gestion afin de vous connecter à iDRAC, puis redirigez le port série du serveur géré vers votre console. Cette fonctionnalité est une alternative à SOL IPMI, qui requiert un utilitaire tel que **solproxy** pour convertir le flux série vers et à partir de paquets réseau.

L'implémentation SOL iDRAC permet de ne pas avoir recours à un utilitaire supplémentaire car la conversion série vers le réseau se produit au sein d'iDRAC.

La console Telnet ou SSH que vous utilisez doit être capable d'interpréter les données issues du port série du serveur géré, et d'y répondre. Le port série se connecte généralement à un environnement qui émule un terminal ANSI- ou VT100-.

Telnet vous permet de vous connecter au port SOL LAN IPMI : le port 2100. La console série est automatiquement redirigée vers votre console Telnet.

Grâce à SSH ou Telnet, vous vous connectez à iDRAC de la même manière qu'à SM-CLP. La redirection SOL peut être démarrée à partir de la cible **/system1/sol1**.

Voir Installation de clients Telnet ou SSH pour plus d'informations sur l'utilisation des clients Telnet et SSH avec iDRAC.

Utilisation de SOL sur Telnet avec HyperTerminal sur Microsoft Windows

1. Sélectionnez **Démarrer**→ **Tous les programmes**→ **Accessoires**→ **Communications**→ **HyperTerminal**.
2. Entrez un nom pour la connexion, choisissez une icône et cliquez sur **OK**.
3. Choisissez **TCP/IP (Winsock)** dans la liste du champ **Connexion en utilisant**.
4. Entrez le nom DNS ou l'adresse IP d'iDRAC dans le champ **Adresse de l'hôte**.
5. Entrez le numéro de port Telnet dans le champ **Numéro de port**.
6. Cliquez sur **OK**.

Pour mettre fin à la session SOL, cliquez sur l'icône de déconnexion HyperTerminal.

Utilisation de SOL sur Telnet avec Linux

Pour démarrer SOL à partir de Telnet sur une station de gestion Linux, suivez ces étapes :

1. Démarrez un environnement.
2. Connectez-vous à iDRAC à l'aide de la commande suivante :

   ```
   telnet <adresse IP iDRAC>
   ```

   REMARQUE : Si vous avez changé le numéro de port par défaut, le port 23, du service Telnet, ajoutez le numéro de port à la fin de la commande **telnet**.

3. Entrez la commande suivante pour démarrer SOL :

   ```
   start /system1/sol1
   ```

   Cette commande vous connecte au port série du serveur géré.

Lorsque vous êtes prêt à quitter SOL, tapez <Ctrl>+] (en maintenant la touche enfoncée et entrez un crochet droit, puis relâchez). Une invite Telnet s'affiche. Tapez quit pour quitter Telnet.

Utilisation de SOL sur SSH

La cible **/system1/sol1** vous permet de rediriger le port série du serveur géré vers votre console SSH.

1. Connectez-vous à iDRAC via OpenSSH ou PuTTY.
2. Entrez la commande suivante pour démarrer SOL :

   ```
   start /system1/sol1
   ```

Cette commande vous connecte au port série du serveur géré. Vous n'avez plus accès aux commandes SM-CLP.

Lorsque vous êtes prêt à quitter la redirection SOL, tapez <Ctrl>+. (en maintenant la touche enfoncée, entrez un point, puis relâchez). La session SSH va se fermer.

Vous ne pouvez pas revenir dans SM-CLP lorsque vous avez démarré SOL. Vous devez quitter la session SSH et en démarrer une nouvelle pour pouvoir utiliser SM-CLP.

Retour à la page du sommaire

Retour à la page du sommaire

Déploiement de votre système d'exploitation via iVM-CLI

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

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

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

Avant de commencer

Avant d'utiliser l'utilitaire iVM-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

- iDRAC est configuré dans chaque système distant.

Exigences du réseau

Un partage réseau doit comprendre les composants suivants :

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

  Le fichier image doit être une image de CD de système d'exploitation ou une image ISO de CD/DVD, avec un format de démarrage standard.

Création d'un fichier image de démarrage

Avant de déployer votre fichier image sur les systèmes distants, assurez-vous qu'un système pris en charge peut être démarré à partir du fichier. Pour tester le fichier image, transférez le fichier image vers un système de test à l'aide de l'interface utilisateur Web iDRAC, 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 (dd) pour créer un fichier image de démarrage pour votre système Linux.

Pour exécuter l'utilitaire, ouvrez une invite de commande et tapez les commandes suivantes :

```
dd if=<périphérique d'entrée> of=<fichier de sortie>
```

Par exemple :

```
dd if=/dev/sdc0 of=mycd.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 un 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 :

   - Suivez les procédures d'installation réseau standard
   - Mettez l'image de déploiement en « lecture seule » pour garantir que chaque système cible démarre et exécute la même procédure de déploiement
4. Effectuez l'une des procédures suivantes :

   - Intégrez **ipmitool** et l'interface de ligne de commande de média virtuel (iVM-CLI) dans votre application de déploiement de système d'exploitation existante. Utilisez l'exemple de script **ivmdeploy** comme guide d'utilisation de l'utilitaire.
   - Utilisez le script **ivmdeploy** existant pour déployer votre système d'exploitation.

Déploiement du système d'exploitation

Utilisez l'utilitaire iVM-CLI et le script **ivmdeploy** inclus avec l'utilitaire pour déployer le système d'exploitation sur vos systèmes distants.

Avant de commencer, vérifiez l'exemple de script **ivmdeploy** inclus avec l'utilitaire iVM-CLI. Le script affiche les étapes détaillées requises pour déployer le système d'exploitation dans les systèmes distants de votre réseau.

La procédure suivante fournit un aperçu de haut niveau du déploiement du système d'exploitation dans les systèmes distants cibles.

1. Répertoriez les adresses IP iDRAC des systèmes distants qui seront déployés dans le fichier texte **ip.txt**, en indiquant une adresse IP par ligne.
2. Insérez un CD ou DVD de système d'exploitation amorçable dans le lecteur de média client.
3. Exécutez **ivmdeploy** à la ligne de commande.

Pour exécuter le script ivmdeploy, entrez la commande suivante à l'invite de commande :

```
ivmdeploy -r ip.txt -u <utilisateur idrac> -p <mot de passe idrac> -c {<image iso9660> | <chemin>}
```

où :

- <*utilisateur idrac*> est le nom d'utilisateur iDRAC, par exemple **root**
- <*mot de passe idrac*> est le mot de passe de l'utilisateur iDRAC, par exemple **calvin**
- <*image iso9660*> est le chemin d'accès à une image ISO9660 du CD ou DVD d'installation du système d'exploitation
- <*chemin*> est le chemin d'accès au périphérique contenant le CD ou DVD d'installation du système d'exploitation

Le script **ivmdeploy** transmet ses options de ligne de commande à l'utilitaire **ivmcli**. Voir Options de ligne de commande pour plus de détails à propos de ces options. Le script traite l'option **-r** de manière légèrement différente de l'option **ivmcli -r**. Si l'argument de l'option **-r** est le nom d'un fichier existant, le script lit les adresses IP iDRAC du fichier spécifié et exécute l'utilitaire **ivmcli** à une seule reprise pour chaque ligne. Si l'argument de l'option **-r** n'est pas un nom de fichier, il doit alors correspondre à l'adresse d'un iDRAC unique. Dans ce cas, l'option **-r** fonctionne comme décrit pour l'utilitaire **ivmcli**.

Le script ivmdeploy prend en charge l'installation uniquement à partir d'un CD/DVD ou d'une image ISO9660 de CD/DVD. Si vous devez procéder à l'installation à partir d'une disquette ou d'une image de disquette, vous pouvez modifier le script pour utiliser l'option **ivmcli -f**.

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

L'utilitaire d'interface de ligne de commande de média virtuel (iVM-CLI) est une interface de ligne de commande inscriptible qui fournit les fonctionnalités de média virtuel de la station de gestion à iDRAC.

L'utilitaire iVM-CLI fournit les fonctionnalités suivantes :

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.

- Les périphériques de média amovibles ou les fichiers image qui sont en accord avec les plug-ins de média virtuel
- L'arrêt automatique lorsque l'option de démarrage unique du micrologiciel iDRAC est activée.
- Les communications sécurisées avec iDRAC à l'aide du protocole Secure Sockets Layer (SSL)

Avant d'exécuter l'utilitaire, assurez-vous que vous disposez des privilèges utilisateur de média virtuel pour pouvoir exécuter iDRAC.

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 iVM-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 droits d'utilisateur privilégié pour pouvoir exécuter l'utilitaire iVM-CLI.

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

Installation de l'utilitaire iVM-CLI

L'utilitaire iVM-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 qui s'affichent à l'écran.

Le CD *Systems Management Consoles* contient les derniers produits Systems Management Software, notamment les diagnostics, 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.

Le CD *Systems Management Consoles* inclut **ivmdeploy**, un modèle de script qui illustre comment utiliser les utilitaires iVM-CLI et RACADM pour déployer le logiciel sur plusieurs systèmes distants.

REMARQUE : Le script **ivmdeploy** dépend des autres fichiers présents dans son répertoire lors de son installation. Si vous souhaitez utiliser le script d'un autre répertoire, vous devez copier tous les fichiers présents dans ce dernier.

Options de ligne de commande

L'interface iVM-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 iDRAC exige la même syntaxe tant pour RACADM que pour les utilitaires iVM-CLI.

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

```
ivmcli [paramètre] [options_d'environnement_de système d'exploitation]
```

La syntaxe de ligne de commande respecte la casse. Voir « Paramètres iVM-CLI » pour plus d'informations.

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

- La connexion iVM-CLI est interrompue pour une raison ou une autre.
- Le processus est manuellement interrompu à l'aide de la commande de système d'exploitation. Par exemple, dans Windows, vous pouvez utiliser le gestionnaire des tâches pour terminer le processus.

Paramètres iVM-CLI

Adresse IP iDRAC

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

Ce paramètre fournit l'adresse IP iDRAC et le port SSL pour lesquels l'utilitaire doit établir une connexion de média virtuel avec l'iDRAC cible. Si vous entrez une adresse IP ou un nom DDNS non valide, un message d'erreur apparaît et la commande est terminée.

<*adresse IP iDRAC*> est une adresse IP unique valide ou le nom DDNS (Dynamic Domain Naming System) iDRAC (si pris en charge). Si le <*port SSL iDRAC*> est omis, le port 443 (port par défaut) est utilisé. À moins que le port SSL par défaut iDRAC n'ait été modifié, le port SSL optionnel n'est pas obligatoire.

Nom d'utilisateur iDRAC

```
-u <nom d'utilisateur iDRAC>
```

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

Le <*nom d'utilisateur iDRAC*> doit avoir les attributs suivants :

- Nom d'utilisateur valide
- Droit d'utilisateur de média virtuel iDRAC

Si l'authentification iDRAC échoue, un message d'erreur s'affiche et la commande se termine.

Mot de passe d'utilisateur iDRAC

`-p <mot de passe d'utilisateur iDRAC>`

Ce paramètre fournit le mot de passe de l'utilisateur iDRAC spécifié.

Si l'authentification iDRAC 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 # 4th partition on device /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.

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)

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 iVM-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 iVM-CLI. Si aucune autre option de non-commutateur n'est fournie, la commande se termine sans erreur.

Affichage manuel

-m

Ce paramètre affiche une « page manuelle » détaillée pour l'utilitaire iVM-CLI, incluant les descriptions de toutes les options possibles.

Données cryptées

-e

Lorsque ce paramètre est inclus dans la ligne de commande, iVM-CLI utilise un canal crypté SSL pour transférer des données entre la station de gestion et iDRAC 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 iVM-CLI

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

- 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 iVM-CLI.

  REMARQUE : L'utilitaire iVM-CLI ne lit pas à partir d'une entrée standard (**stdin**). Par conséquent, la redirection **stdin** n'est pas exigée.

- Exécution en arrière-plan : par défaut, l'utilitaire iVM-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 iVM-CLI (le cas échéant, le script serait bloqué jusqu'à ce que le programme iVM-CLI soit terminé). Lorsque plusieurs instances iVM-CLI sont démarrées de cette manière et qu'une ou plusieurs instances de commande doivent être terminées manuellement, utilisez les équipements spécifiques au système d'exploitation pour répertorier et terminer les processus.

Codes de retour iVM-CLI

0 = aucune erreur

1 = connexion impossible

2 = erreur de ligne de commande iVM-CLI

3 = la connexion du micrologiciel 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.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de l'utilitaire de configuration iDRAC

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Présentation générale

L'utilitaire de configuration iDRAC est un environnement de configuration de prédémarrage vous permettant d'afficher et de définir les paramètres d'iDRAC et du serveur géré. Vous pouvez notamment :

- Afficher les numéros de révision du micrologiciel pour iDRAC et le micrologiciel de fond de panier principal
- Configurer, activer ou désactiver le réseau local iDRAC
- Activer ou désactiver IPMI sur le LAN
- Activer une destination d'interruption d'événements sur plateforme (PET) LAN
- Connecter ou déconnecter les périphériques de média virtuel
- Changer le nom d'utilisateur et le mot de passe d'administration
- Rétablir les paramètres d'usine de la configuration iDRAC
- Afficher les messages du journal des événements système (SEL) ou effacer les messages du journal

Les tâches que vous pouvez effectuer à l'aide de l'utilitaire de configuration iDRAC peuvent également être effectuées via d'autres utilitaires fournis par iDRAC ou le logiciel OpenManage, notamment l'interface Web, l'interface de ligne de commande SM-CLP, l'interface de ligne de commande RACADM locale et, dans le cas de la configuration réseau de base, sur l'écran LCD CMC lors de la configuration CMC initiale.

Démarrage de l'utilitaire de configuration iDRAC

Vous devez utiliser une console connectée à iKVM pour accéder initialement à l'utilitaire de configuration iDRAC ou après une réinitialisation des paramètres par défaut d'iDRAC.

1. Sur le clavier connecté à la console iKVM, appuyez sur <Impr. écran> pour afficher le menu OSCAR (On Screen Configuration and Reporting) iKVM. Utilisez la <flèche vers le haut> et la <flèche vers le bas> pour mettre en surbrillance le logement contenant votre serveur, puis appuyez sur <Entrée>.
2. Mettez sous tension ou redémarrez le serveur en appuyant sur le bouton d'alimentation situé à l'avant du serveur.
3. Lorsque le message **Appuyez sur <Ctrl-E> pour configurer l'accès à distance dans 5 sec.....** s'affiche, appuyez immédiatement sur <Ctrl><E>.

REMARQUE : Si votre système d'exploitation commence à se charger avant d'appuyer sur <Ctrl><E>, laissez le système terminer son démarrage, puis redémarrez votre serveur et réessayez.

L'utilitaire de configuration iDRAC s'affiche. Les deux premières lignes fournissent des informations sur le micrologiciel iDRAC et les révisions du micrologiciel du fond de panier principal. Les niveaux de révision peuvent être utiles afin de déterminer si une mise à niveau du micrologiciel est nécessaire.

Le micrologiciel iDRAC est la partie du micrologiciel s'articulant autour des interfaces externes, telles que l'interface Web, les interfaces SM-CLP et Web. Le micrologiciel de fond de panier principal est la partie du micrologiciel qui s'interface avec l'environnement matériel du serveur et qui le surveille.

Utilisation de l'utilitaire de configuration iDRAC

Sous les messages de révision du micrologiciel, le reste de l'utilitaire de configuration iDRAC se compose d'un menu d'éléments auxquels vous pouvez accéder à l'aide de la <flèche vers le haut> et de la <flèche vers le bas>.

- Si un élément de menu renvoie à un sous-menu ou à un champ de texte modifiable, appuyez sur <Entrée> pour accéder à l'élément et sur <Échap> pour le quitter une fois sa configuration terminée.
- Si des valeurs sélectionnables telles que Oui/Non ou Activé/Désactivé sont associées à un élément, appuyez sur la <flèche gauche>, la <flèche droite> ou sur <Espace> pour choisir une valeur.
- Si un élément n'est pas modifiable, il apparaît en bleu. Certains éléments deviennent modifiables en fonction des autres sélections que vous effectuez.
- La dernière ligne de l'écran affiche des instructions concernant l'élément actuel. Vous pouvez appuyer sur <F1> pour afficher l'aide sur l'élément actuel.
- Lorsque vous avez fini d'utiliser l'utilitaire de configuration iDRAC, appuyez sur <Échap> pour afficher le menu Quitter, dans lequel vous pouvez choisir d'enregistrer ou d'ignorer vos modifications, ou encore de retourner dans l'utilitaire.

Les sections suivantes décrivent les éléments de menu de l'utilitaire de configuration iDRAC.

LAN

Utilisez la <flèche gauche>, la <flèche droite> et la barre d'espace pour choisir entre **Activé** et **Désactivé**.

Le LAN iDRAC est désactivé dans la configuration par défaut. Le LAN doit être activé pour permettre l'utilisation des services iDRAC, comme par exemple l'interface Web, l'accès Telnet/SSH à l'interface de ligne de commande SM-CLP, la redirection de console et le média virtuel.

Si vous choisissez de désactiver le LAN, l'avertissement suivant s'affiche :

```
iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.

(L'interface hors bande iDRAC sera désactivée si le canal LAN est désactivé.)

Appuyez sur n'importe quelle touche pour effacer le message et continuer.
```

Le message vous informe que, outre les services auxquels vous accédez en vous connectant directement aux ports iDRAC HTTP, HTTPS, Telnet ou SSH, le trafic réseau de gestion hors bande, tels que les messages IPMI envoyés à iDRAC à partir d'une station de gestion, n'est pas reçu lorsque le LAN est désactivé. L'interface RACADM locale reste disponible et peut être utilisée pour reconfigurer le LAN iDRAC.

IPMI sur le LAN (act./dés.)

Appuyez sur la <flèche gauche>, la <flèche droite> et la barre d'espace pour choisir entre **Activé** et **Désactivé**. Lorsque **Désactivé** est sélectionné, iDRAC n'accepte pas les messages IPMI en provenance de l'interface LAN.

Si vous sélectionnez **Désactivé**, l'avertissement suivant s'affiche :

```
iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.

(L'interface hors bande iDRAC sera désactivée si le canal LAN est désactivé.)
```

Appuyez sur n'importe quelle touche pour effacer le message et continuer. Voir LAN pour obtenir une explication du message.

Paramètres LAN

Appuyez sur <Entrée> pour afficher le sous-menu Paramètres LAN. Une fois la configuration des paramètres LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

Tableau 12-1. Paramètres LAN

Élément	Description
Clé de cryptage RMCP+	Appuyez sur <Entrée> pour modifier la valeur et sur <Échap> lorsque vous avez terminé. La clé de cryptage RMCP+ est une chaîne hexadécimale de 40 caractères (caractères 0-9, a-f et A-F). RMCP+ est une extension IPMI qui ajoute de l'authentification et du cryptage à IPMI. La valeur par défaut est une chaîne de 40 0s.
Source d'adresse IP	Choisissez entre **DHCP** et **Statique**. Lorsque DHCP est sélectionné, les champs **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut** sont obtenus auprès d'un serveur DHCP. Si aucun serveur DHCP n'est trouvé sur le réseau, les champs sont définis sur zéro. Lorsque **Statique** est sélectionné, les éléments **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut** deviennent modifiables**.**
Adresse IP Ethernet	Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP obtenue auprès de DHCP. Si la **source d'adresse IP** est définie sur **Statique**, entrez l'adresse IP que vous souhaitez attribuer à iDRAC. L'adresse par défaut est **192.168.0.120** plus le numéro du logement contenant le serveur.
Adresse MAC	Il s'agit de l'adresse MAC non modifiable de l'interface réseau iDRAC.
Masque de sous-réseau	Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse de masque de sous-réseau obtenue auprès de DHCP. Si la **source d'adresse IP** est définie sur **Statique**, entrez le masque de sous-réseau d'iDRAC. L'adresse par défaut est **255.255.255.0**.
Passerelle par défaut	Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP. Si la **source d'adresse IP** est définie sur **Statique**, entrez l'adresse IP de la passerelle par défaut. L'adresse par défaut est **192.168.0.1**.
Alerte LAN activée	Sélectionnez **Activé** pour activer l'alerte d'interruption d'événements sur plateforme (PET) LAN.
Entrée 1 de règle d'alerte	Sélectionnez Activer ou Désactiver pour activer la première destination de l'alerte.
Destination de l'alerte 1	Entrez l'adresse IP à laquelle les alertes LAN PET seront transférées.
Chaîne de nom d'hôte	Appuyez sur <Entrée> pour modifier. Entrez le nom de l'hôte des alertes PET.
Serveurs DNS	Sélectionnez **Activé** pour récupérer les adresses de serveur DNS auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** pour

de DHCP	spécifier les adresses de serveur DNS ci-dessous.
Serveur DNS 1	Si **Serveurs DNS de DHCP** est **désactivé**, entrez l'adresse IP du premier serveur DNS.
Serveur DNS 2	Si **Serveurs DNS de DHCP** est **désactivé**, entrez l'adresse IP du deuxième serveur DNS.
Enregistrer le nom iDRAC	Sélectionnez **Activé** pour enregistrer le nom iDRAC dans le service DNS. Sélectionnez **Désactivé** si vous ne voulez pas que les utilisateurs puissent accéder au nom iDRAC dans DNS.
Nom iDRAC	Si **Enregistrer le nom iDRAC** est défini sur **Activé**, appuyez sur <Entrée> pour modifier le champ de texte **Nom iDRAC DNS actuel**. Appuyez sur <Entrée> une fois la modification du nom iDRAC terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom iDRAC doit être un nom d'hôte DNS valide.
Nom de domaine de DHCP	Sélectionnez **Activé** si vous souhaitez obtenir le nom de domaine auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** si vous souhaitez spécifier le nom de domaine.
Nom de domaine	Si **Nom de domaine de DHCP** est **désactivé**, appuyez sur <Entrée> pour modifier le champ de texte **Nom de domaine actuel**. Appuyez sur <Entrée> une fois la modification terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom de domaine doit être un domaine DNS valide, par exemple `monentreprise.com`.

Média virtuel

Utilisez la <flèche gauche> et la <flèche droite> pour sélectionner **Connecté** ou **Déconnecté**. Lorsque vous sélectionnez **Connecté**, les périphériques de média virtuel sont connectés au bus USB, ce qui les rend disponibles lors des sessions de **redirection de console**.

Si vous sélectionnez **Déconnecté**, les utilisateurs ne peuvent pas accéder aux périphériques de média virtuel lors des sessions de **redirection de console**.

REMARQUE : Pour utiliser un lecteur Flash USB avec la fonctionnalité **Média virtuel**, le **type d'émulation de lecteur Flash USB** doit être défini sur **Disque dur** dans l'utilitaire de configuration du BIOS. L'utilitaire de configuration du BIOS est accessible en appuyant sur <F2> lors du démarrage du serveur. Si le **type d'émulation de lecteur Flash USB** est défini sur **Automatique**, le lecteur Flash apparaît sous forme de lecteur de disquette sur le système.

Configuration utilisateur LAN

L'utilisateur LAN est le compte administrateur iDRAC, soit **root** par défaut. Appuyez sur <Entrée> pour afficher le sous-menu Configuration utilisateur LAN. Une fois la configuration de l'utilisateur LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

Tableau 12-2. Page Configuration utilisateur LAN

Élément	Description
Accès au compte	Sélectionnez **Activé** pour activer le compte administrateur. Sélectionnez **Désactivé** pour désactiver le compte administrateur.
Privilèges de compte	Choisissez entre **Administrateur**, **Utilisateur**, **Opérateur** et **Aucun accès**.
Nom d'utilisateur de compte	Appuyez sur <Entrée> pour modifier le nom d'utilisateur et appuyez sur <Échap> lorsque vous avez terminé. Le nom d'utilisateur par défaut est **root**.
Entrer le mot de passe	Tapez le nouveau mot de passe du compte administrateur. Les caractères ne sont pas renvoyés sur l'affichage lorsque vous les tapez.
Confirmer le mot de passe	Retapez le nouveau mot de passe du compte administrateur. Si les caractères que vous avez entrés ne correspondent pas à ceux que vous avez tapés dans le champ **Entrer le mot de passe**, un message s'affiche et vous devez entrer à nouveau le mot de passe.

Rétablir les paramètres par défaut

Utilisez l'élément de menu **Rétablir les paramètres par défaut** pour rétablir les paramètres d'usine de tous les éléments de la configuration iDRAC. Cette opération peut être requise, par exemple, si vous avez oublié le mot de passe utilisateur d'administration ou si vous souhaitez reconfigurer iDRAC à partir des paramètres par défaut.

REMARQUE : Dans la configuration par défaut, la mise en réseau iDRAC est désactivée. Vous ne pouvez pas reconfigurer iDRAC sur le réseau tant que vous n'avez pas activé le réseau iDRAC dans l'utilitaire de configuration iDRAC.

Appuyez sur <Entrée> pour sélectionner l'élément. Le message d'avertissement suivant apparaît :

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >

(Le rétablissement des paramètres d'usine va restaurer les paramètres utilisateur non volatiles. Voulez-vous continuer ?

< NO (Annuler) >

< YES (Continuer)) >
```

Sélectionnez **YES** et appuyez sur <Entrée> pour rétablir les paramètres par défaut d'iDRAC.

Menu Journal des événements système

Le menu **Journal des événements système** vous permet d'afficher les messages du journal des événements système (SEL) et d'effacer les messages du journal. Appuyez sur <Entrée> pour afficher le menu **Journal des événements système**. Le système compte les entrées de journal, puis affiche le nombre total d'enregistrements et le message le plus récent. Le journal SEL conserve un maximum de 512 messages.

Pour afficher les messages du journal SEL, sélectionnez **Afficher le journal des événements système** et appuyez sur <Entrée>. Utilisez la <flèche gauche> pour accéder au message précédent (plus ancien) et la <flèche droite> pour accéder au message suivant (plus récent). Entrez un nombre d'enregistrement pour atteindre cet enregistrement. Appuyez sur <Échap> lorsque vous avez fini d'afficher les messages du journal SEL.

REMARQUE : Vous pouvez uniquement effacer les messages du journal SEL dans l'utilitaire de configuration iDRAC ou dans l'interface Web iDRAC.

Pour effacer les messages du journal SEL, sélectionnez **Effacer le journal des événements système** et appuyez sur <Entrée>.

Lorsque vous avez fini d'utiliser le menu Journal SEL, appuyez sur <Échap> pour revenir au menu précédent.

Sortie de l'utilitaire de configuration iDRAC

Lorsque vous avez fini d'apporter des modifications à la configuration iDRAC, appuyez sur la touche <Échap> pour afficher le menu Quitter.

Sélectionnez **Enregistrer les modifications et quitter** et appuyez sur <Entrée> pour conserver vos modifications.

Sélectionnez **Ignorer les modifications et quitter** et appuyez sur <Entrée> pour ignorer les modifications que vous avez apportées.

Sélectionnez **Retour au programme d'installation** et appuyez sur <Entrée> pour revenir dans l'utilitaire de configuration iDRAC.

Retour à la page du sommaire

Retour à la page du sommaire

Récupération et dépannage du serveur géré

Guide d'utilisation du micrologiciel Integrated Dell™ Remote Access Controller, version 1.00

Cette section explique comment effectuer les tâches relatives au diagnostic et au dépannage d'un serveur géré distant à l'aide des services iDRAC. Elle contient les sous-sections suivantes :

- Indications concernant les problèmes : vous aide à rechercher les messages et d'autres indications système en vue d'établir un diagnostic du problème
- Outils de résolution des problèmes : décrit les outils iDRAC que vous pouvez utiliser pour dépanner votre système
- Dépannage et questions les plus fréquentes : répond aux situations types que vous êtes susceptibles de rencontrer

---

La sécurité d'abord : pour vous et votre système

Pour effectuer certaines procédures de cette section, vous devez utiliser le châssis, le serveur PowerEdge ou d'autres modules de matériel. N'essayez pas de réparer le matériel du système par vous-même. Tenez-vous en aux explications fournies dans ce guide et dans votre documentation système.

⚠ **PRÉCAUTION : De nombreuses réparations peuvent être uniquement effectuées par un technicien d'entretien certifié. Vous êtes uniquement autorisé à effectuer les opérations de dépannage et les simples réparations conformément aux spécifications de votre documentation produit ou conformément aux instructions qui vous sont fournies en ligne, par téléphone et par l'équipe de support. Tout endommagement résultant d'une réparation non autorisée par Dell n'est pas couverte par votre garantie. Lisez et suivez les consignes de sécurité fournies avec le produit.**

Voyants inhérents aux problèmes

Cette section décrit les indications concernant les problèmes susceptibles de se produire sur votre système.

Voyants LED

Le signalement initial de tout problème sur le système peut se faire via les LED présentes sur le châssis ou les composant installés dans le châssis. Les composants et modules suivants sont dotés de LED de condition :

- Écran LCD du châssis
- Serveurs
- Ventilateurs
- CMC
- Modules d'E/S
- Blocs d'alimentation

La LED unique sur l'écran LCD du châssis résume la condition de tous les composants du système. Une LED bleue unie sur l'écran LCD indique qu'aucune condition d'anomalie n'a été détectée sur le système. Une LED orange qui clignote sur l'écran LCD indique qu'une ou plusieurs conditions d'anomalie ont été détectées.

Si une LED orange clignote sur l'écran LCD du châssis, vous pouvez utiliser le menu d'écran LCD pour localiser le composant présentant une anomalie. Voir le *Guide d'utilisation du micrologiel Dell CMC, version 1.0* pour obtenir de l'aide concernant l'utilisation de l'écran LCD.

Le tableau 13-1 décrit les significations de la LED sur le serveur PowerEdge :

Tableau 13-1. Voyants LED du serveur

Voyant LED	Signification
vert uni	Le serveur est sous tension. L'absence de LED verte signifie que le serveur n'est pas sous tension.
bleu uni	iDRAC est intègre.
orange clignotant	iDRAC a détecté une condition d'anomalie ou s'apprête à mettre à jour le micrologiciel.
bleu clignotant	Un utilisateur a activé la référence de l'indicateur d'emplacement pour ce serveur.

Voyants inhérents aux problèmes du matériel

Les indications de problèmes du matériel sur un module sont les suivantes :

- Échec de la mise sous tension
- Ventilateurs bruyants
- Perte de connectivité réseau
- Alertes de batterie, de température, de tension ou de capteur de contrôle de l'alimentation
- Pannes de disque dur
- Panne du média USB
- Endommagement physique provoqué par une chute, de l'eau ou toute autre contrainte externe

Lorsque ces types de problèmes se produisent, vous pouvez essayer de corriger le problème à l'aide des stratégies suivantes :

- Repositionnez le module et redémarrez-le
- Essayez d'insérer le module dans une baie différente du châssis
- Essayez de remplacer les disques durs ou les clés USB
- Reconnectez ou remplacez les câbles d'alimentation et réseau

Si ces étapes ne permettent pas de corriger le problème, consultez le *Manuel du propriétaire du matériel* pour obtenir des informations de dépannage spécifiques concernant le périphérique matériel.

Autres voyants inhérents aux problèmes

Tableau 13-2. Voyants inhérents aux problèmes

Recherchez :	Action :
Messages d'alerte de Systems Management Software	Consultez la documentation relative à Systems Management Software.
Messages dans le journal des événements système	Voir Vérification du journal des événements système (SEL)
Messages dans les codes du POST de démarrage	Voir Vérification des codes du POST.
Messages sur l'écran de la dernière panne	Voir Affichage de l'écran de la dernière panne système
Messages dans le journal iDRAC	Voir Affichage du journal iDRAC.

Outils de résolution des problèmes

Cette section décrit les services iDRAC que vous pouvez utiliser pour diagnostiquer des problèmes sur votre système, notamment lorsque vous essayez de les résoudre à distance.

- Vérification de l'intégrité du système
- Vérification des messages d'erreur dans le journal des événements système
- Vérification des codes du POST
- Affichage de l'écran de la dernière panne
- Affichage du journal iDRAC
- Accès aux informations sur le système
- Identification du serveur géré dans le châssis
- Utilisation de la console de diagnostics
- Gestion de l'alimentation d'un système distant

Vérification de l'intégrité du système

Lorsque vous vous connectez à l'interface Web iDRAC, la première page qui s'affiche décrit l'intégrité des composants système. Le tableau 13-3 décrit la signification des voyants d'intégrité du système.

Tableau 13-3. Voyants d'intégrité du système

Voyant	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.

Cliquez sur un composant quelconque de la page **Intégrité** pour afficher les informations sur ce composant. Les lectures de capteur s'affichent pour les batteries, les températures, les tensions et le contrôle de l'alimentation, vous aidant ainsi à diagnostiquer certains types de problèmes. Les pages d'informations iDRAC et CMC contiennent des informations utiles sur la configuration et la condition actuelles.

Vérification du journal des événements système (SEL)

La page **Journal SEL** affiche les messages des événements qui se produisent sur le serveur géré.

Pour afficher le **journal des événements système**, effectuez les étapes suivantes :

1. Cliquez sur **Système**, puis sur l'onglet **Journaux**.
2. Cliquez sur **Journal des événements système** pour afficher la page **Journal des événements système**.

   La page **Journal des événements système** affiche un voyant d'intégrité système (voir le tableau 13-3), un horodateur et une description de l'événement.
3. Cliquez sur le bouton approprié de la page **Journal des événements système** pour continuer (voir Tableau 13-4).

Tableau 13-4. 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**.

Vérification des codes du POST

La page **Codes du POST** affiche le dernier code de POST du système avant le démarrage du système d'exploitation. Les codes du POST sont les indicateurs de progression du BIOS système, indiquant les diverses étapes de la séquence d'amorçage suite à une mise sous tension et vous permettent de diagnostiquer les erreurs de démarrage du système.

REMARQUE : Affichez le texte pour rechercher les numéros de message du code du POST sur l'écran LCD ou dans le *Manuel du propriétaire du matériel.*

Pour afficher les codes du POST, effectuez les étapes suivantes :

1. Cliquez sur **Système**, cliquez sur l'onglet **Journaux**, puis sur **Codes du POST**.

   La page **Codes du POST** affiche un voyant d'intégrité système (voir le tableau 13-3), un code hexadécimal et une description du code.
2. Cliquez sur le bouton approprié de la page **Code du POST** pour continuer (voir Tableau 13-5).

Tableau 13-5. Boutons du code du POST

Bouton	Action
Imprimer	Imprime la page **Codes du POST**.
Actualiser	Recharge la page **Codes du POST**.

Affichage de l'écran de la dernière panne système

AVIS : La fonctionnalité Écran de la dernière panne doit être configurée dans Server Administrator et dans l'interface Web iDRAC. Voir Configuration du serveur géré pour la saisie de l'écran de la dernière panne pour obtenir des instructions sur la configuration de 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. L'image de la dernière panne du système est enregistrée dans le magasin permanent d'iDRAC et est accessible à distance.

Pour afficher la page **Écran de la dernière panne**, effectuez les étapes suivantes :

- Cliquez sur **Système**, cliquez sur l'onglet **Journaux**, puis sur **Dernière panne**.

La page **Écran de la dernière panne** inclut les boutons présentés dans le tableau 13-6 :

REMARQUE : Les boutons **Enregistrer** et **Supprimer** n'apparaissent pas en l'absence d'écran de panne enregistré.

Tableau 13-6. 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 la page **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 configurée avec une valeur trop élevée. La valeur par défaut est 480 secondes. Utilisez Server Administrator ou IT Assistant pour définir l'horloge de réinitialisation du système sur 60 secondes et s'assurer que la fonctionnalité **Écran de la dernière panne** fonctionne correctement. Voir Configuration du serveur géré pour la saisie de l'écran de la dernière panne pour obtenir des informations supplémentaires.

Affichage du journal iDRAC

Le **journal iDRAC** est un journal permanent conservé dans le micrologiciel iDRAC. 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 iDRAC. Les entrées les plus anciennes sont effacées quand le journal est plein.

Tandis que le **journal des événements système** (SEL) contient des enregistrements d'événements qui se produisent dans le serveur géré, le **journal iDRAC** contient des enregistrements d'événements qui se produisent dans iDRAC.

Pour accéder au journal **iDRAC**, effectuez les étapes suivantes :

- Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis cliquez sur **Journal iDRAC**.

Le **journal iDRAC** fournit les informations répertoriées au tableau 13-7.

Tableau 13-7. Informations sur la page Journal iDRAC

Champ	Description
Date et heure	Date et heure en anglais (par exemple, Dec 19 16:55:47). iDRAC définit son horloge en fonction de l'horloge du serveur géré. Si iDRAC ne peut pas communiquer avec le serveur géré lors de son premier démarrage, l'heure affichée est celle du démarrage du système sous forme de chaîne.
Source	L'interface à l'origine de l'événement.
Description	Description brève de l'événement et nom d'utilisateur qui s'est connecté à iDRAC.

Utilisation des boutons de la page Journal iDRAC

La page **Journal iDRAC** dispose des boutons suivants (voir le tableau 13-8).

Tableau 13-8. Boutons du journal iDRAC

Bouton	Action
Imprimer	Imprime la page **Journal iDRAC**.
Effacer le journal	Efface les entrées du **journal iDRAC**. **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 iDRAC** 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 iDRAC**.

Affichage des informations sur le système

La page **Résumé du système** affiche des informations sur les composants système suivants :

- Enceinte principale du système
- Integrated Dell Remote Access Controller

Pour accéder aux informations sur le système, cliquez sur **Système**→ **Propriétés**.

Enceinte principale du système

Le tableau 13-9 et le tableau 13-10 décrivent les propriétés de l'enceinte principale du système.

Tableau 13-9. Champs d'Informations sur le système

Champ	Description
Description	Fournit une description du système.
Version du BIOS	Indique la version du BIOS du système.
Numéro de service	Indique le numéro de service du système.
Nom d'hôte	Indique le nom du système hôte.
Nom du système d'exploitation	Indique le système d'exploitation fonctionnant sur le système.

Tableau 13-10. Champs de récupération automatique

Champ	Description
Action de récupération	Lorsqu'un *arrêt imprévu du système* est détecté, iDRAC peut être configuré pour exécuter l'une des actions suivantes : **Pas d'action**, **Réinitialisation matérielle**, **Mise hors tension** ou **Cycle d'alimentation**.
Compte à rebours initial	Le nombre de secondes écoulées après la détection d'un *arrêt imprévu du système* avant qu'iDRAC n'effectue une action de récupération.
Compte à rebours actuel	La valeur actuelle, en secondes, de la minuterie du compte à rebours.

Integrated Dell Remote Access Controller

Le tableau 13-11 décrit les propriétés iDRAC.

Tableau 13-11. Champs d'informations iDRAC

Champ	Description
Date et heure	Indique la date et l'heure actuelles sur iDRAC en GMT.
Version du micrologiciel	Indique la version du micrologiciel iDRAC.
Micrologiciel mis à jour	Indique la date de la dernière mise à jour du micrologiciel. La date est affichée au format UTC, par exemple : Mar 8 mai 2007, 22:18:21 UTC.
Adresse IP	Adresse à 32 bits qui identifie l'interface réseau. La valeur est affichée au format *séparé par un point* , tel que 143.166.154.127.
Passerelle	Adresse IP de la passerelle qui agit comme un pont entre les autres réseaux. La valeur est au format *séparé par un point*, tel que 143.166.150.5.
Masque de sous-réseau	Masque de sous-réseau qui identifie les parties de l'adresse IP constituant le préfixe du réseau étendu et le numéro d'hôte. La valeur est affichée au format *séparé par un point* , tel que 255.255.0.0.
Adresse MAC	Adresse MAC (Media Access Control) qui identifie de manière unique chaque NIC sur un réseau, par exemple 00-00-0c-ac-08. Il s'agit d'une référence attribuée par Dell qui ne peut pas être modifiée.
Protocole DHCP activé	**Activé** indique que le protocole de configuration dynamique d'hôte (DHCP) est activé. **Désactivé** indique que le protocole DHCP n'est *pas* activé.

Identification du serveur géré dans le châssis

Le châssis PowerEdge M1000-e peut contenir jusqu'à seize serveurs. Pour rechercher un serveur spécifique dans le châssis, vous pouvez utiliser l'interface Web iDRAC pour activer une LED bleue qui clignote sur le serveur. Lorsque vous activez la LED, vous pouvez spécifier le nombre de secondes au cours desquelles vous souhaitez que la LED clignote afin de vous assurer que vous pouvez atteindre le châssis alors que la LED clignote toujours. Si vous entrez 0, la LED clignote tant que vous ne l'avez pas désactivée.

Pour identifier le serveur :

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Dépannage**.
2. Sur la page **Identifier**, cochez la case de valeur située en regard de **Identifier le serveur**.
3. Dans le champ **Délai d'attente d'identification du serveur**, entrez le nombre de secondes pendant lesquelles la LED doit clignoter. Entrez 0 si vous souhaitez que la LED clignote jusqu'à ce que vous la désactiviez.
4. Cliquez sur **Appliquer**.

Une LED bleue présente sur le serveur clignote pour le nombre de secondes que vous avez spécifié.

Si vous avez entré 0 pour laisser la LED clignoter, suivez ces étapes pour la désactiver :

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Dépannage**.
2. Sur la page **Identifier**, décochez la case de valeur située en regard de **Identifier le serveur**.
3. Cliquez sur **Appliquer**.

Utilisation de la console de diagnostics

iDRAC fournit un ensemble standard d'outils de diagnostic réseau (voir Tableau 13-12) qui sont semblables aux outils fournis avec les systèmes Microsoft® Windows® ou Linux. À l'aide de l'interface Web iDRAC, vous pouvez accéder aux outils de débogage réseau.

Pour accéder à la page **Console de diagnostics**, effectuez les étapes suivantes :

1. Cliquez sur **Système**→ **iDRAC**→ **Dépannage**.
2. Cliquez sur l'onglet **Diagnostic**.

Le tableau 13-12 décrit les commandes qui peuvent être entrées sur la page **Console de diagnostics**. Tapez une commande et cliquez sur **Envoyer**. Les résultats du débogage apparaissent sur la page **Console de diagnostics**.

Cliquez sur le bouton **Effacer** pour effacer les résultats affichés par la commande précédente.

Pour actualiser la page **Console de diagnostics**, cliquez sur **Actualiser**.

Tableau 13-12. 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 du tableau de l'interface réseau.
netstat	Imprime le contenu du tableau de routage.
ping *<Adresse IP>*	Vérifie que l'adresse IP de destination est accessible à partir d'iDRAC avec le contenu actuel du tableau de routage. Il faut saisir une adresse IP de destination dans le champ à droite de cette option. Un paquet d'écho du protocole de contrôle des messages sur Internet (ICMP) est envoyé à l'adresse IP de destination en fonction du contenu de la table de routage utilisée.
gettracelog	Affiche le journal de suivi iDRAC. Voir gettracelog pour des informations supplémentaires.

Gestion de l'alimentation d'un système distant

iDRAC vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance sur un serveur géré. Utilisez la page Gestion de l'alimentation pour réaliser un arrêt méthodique du système d'exploitation lors des redémarrages et des mises sous tension et hors tension.

REMARQUE : Vous devez avoir le droit d'**exécuter les commandes d'action du serveur** pour effectuer les actions de gestion de l'alimentation. Voir Ajout et configuration des utilisateurs iDRAC pour obtenir de l'aide concernant la configuration des droits d'utilisateur.

1. Cliquez sur **Système**, puis sur l'onglet **Gestion de l'alimentation**.
2. Sélectionnez une **action de contrôle de l'alimentation**, par exemple **Réinitialiser le système (redémarrage à chaud)**.

Le tableau 13-13 fournit des informations sur les actions de contrôle de l'alimentation.

3. Cliquez sur **Appliquer** pour effectuer l'action sélectionnée.

4. Cliquez sur le bouton approprié pour continuer. Voir tableau 13-14.

Tableau 13-13. Actions de contrôle de l'alimentation

Allumer le système	Met le système sous tension (comme si vous appuyiez sur le bouton d'alimentation lorsque le système est hors tension).
Arrêter le système	Met le système hors tension (comme si vous appuyiez sur le bouton d'alimentation lorsque le système est sous tension).
NMI (interruption non masquable)	Envoie une interruption de niveau élevé au système d'exploitation, qui par conséquent arrête les opérations pour permettre des activités de diagnostic ou de dépannage critiques.
Arrêt normal	Tente d'arrêter le système d'exploitation correctement, puis met hors tension le système. Ceci nécessite que le système d'exploitation prenne en charge l'interface ACPI afin de contrôler la gestion de l'alimentation système.
Réinitialiser le système (redémarrage à chaud)	Redémarre le système sans le mettre hors tension (redémarrage à chaud).
Exécuter un cycle d'alimentation sur le système	Met le système hors tension, puis le redémarre (redémarrage à froid).

Tableau 13-14. Boutons de la page Gestion de l'alimentation

Bouton	Action
Imprimer	Imprime les valeurs de **Gestion de l'alimentation** qui apparaissent à l'écran.
Actualiser	Recharge la page **Gestion de l'alimentation**.
Appliquer	Enregistre les nouveaux paramètres que vous créez pendant l'affichage de la page Gestion de l'alimentation.

Dépannage et questions les plus fréquentes

Le tableau 13-15 contient les questions les plus fréquentes sur les problèmes de dépannage.

Tableau 13-15. Questions les plus fréquentes/Dépannage

Question	Réponse
La LED présente sur le serveur clignote en orange.	Vérifiez les messages du journal SEL, puis effacez-les pour arrêter la LED qui clignote. Depuis l'interface Web iDRAC : • Voir Vérification du journal des événements système (SEL) À partir de la commande SM-CLP : • Voir Gestion SEL À partir de l'utilitaire de configuration iDRAC : • Voir le menu Menu Journal des événements système
Une LED bleue clignote sur le serveur.	Un utilisateur a activé la référence de l'indicateur d'emplacement pour le serveur. Il s'agit d'un signal leur permettant d'identifier le serveur dans le châssis. Voir Identification du serveur géré dans le châssis pour plus d'informations sur cette fonctionnalité.
Comment puis-je trouver l'adresse IP d'iDRAC ?	Depuis l'interface Web CMC : 1. Cliquez sur **Châssis**→ **Serveurs**, puis sur l'onglet **Configuration**. 2. Cliquez sur **Déployer**. 3. Lisez l'adresse IP de votre serveur dans le tableau affiché. À partir d'iKVM : • Redémarrez le serveur et entrez dans l'utilitaire de configuration iDRAC en appuyant sur <Ctrl><E> OU • Surveillez l'affichage de l'adresse IP lors du POST du BIOS. OU • Sélectionnez la console « Dell CMC » dans OSCAR afin de vous connecter à CMC via une connexion série locale. Les commandes RACADM CMC peuvent être émises à partir de cette connexion. Reportez-vous au *Guide d'utilisation du micrologiel CMC, version 1.0* pour accéder à la liste complète des sous-

	commandes RACADM CMC.

Comment puis-je trouver l'adresse IP d'iDRAC ? *(suite)*	Par exemple :
	
	`$ racadm getniccfg -m server-1`
	
	`DHCP Enabled = 1`
	`IP Address = 192.168.0.1`
	`Subnet Mask = 255.255.255.0`
	`Gateway = 192.168.0.1`
	
	À partir d'une commande RACADM locale :
	
	1. Entrez la commande suivante à l'invite de commande :
	
	`racadm getsysinfo`
	
	À partir de l'écran LCD :
	
	1. Sur le menu principal, mettez en surbrillance **Serveur** et appuyez sur le bouton de vérification.
	2. Sélectionnez le serveur dont vous recherchez l'adresse IP et appuyez sur le bouton de vérification.

Comment puis-je trouver l'adresse IP de CMC ?	Depuis l'interface Web iDRAC :
	
	• Cliquez sur **Système**→ **Accès à distance**→ **CMC**.
	
	L'adresse IP CMC s'affiche sur la page **Résumé**.
	
	OU
	
	• Sélectionnez la console « Dell CMC » dans OSCAR afin de vous connecter à CMC via une connexion série locale. Les commandes RACADM CMC peuvent être émises à partir de cette connexion. Reportez-vous au *Guide d'utilisation du micrologiel CMC, version 1.0* pour accéder à la liste complète des sous-commandes RACADM CMC.
	
	`$ racadm getniccfg -m chassis`
	
	`NIC Enabled = 1`
	`DHCP Enabled = 1`
	`Static IP Address = 192.168.0.120`
	`Static Subnet Mask = 255.255.255.0`
	`Static Gateway = 192.168.0.1`
	`Current IP Address = 10.35.155.151`
	`Current Subnet Mask = 255.255.255.0`
	`Current Gateway = 10.35.155.1`
	`Speed = Autonegotiate`
	`Duplex = Autonegotiate`

La connexion réseau iDRAC ne fonctionne pas.	• Assurez-vous que le câble LAN est connecté à CMC. • Assurez-vous que le LAN iDRAC est activé.
J'ai inséré le serveur dans le châssis et j'ai appuyé sur le bouton d'alimentation, mais rien ne s'est produit.	• iDRAC nécessite environ 30 secondes pour s'initialiser avant la mise sous tension du serveur. Patientez 30 secondes et appuyez de nouveau sur le bouton d'alimentation. • Vérifiez le bilan de puissance CMC. Le bilan de puissance du châssis a peut-être été dépassé.
J'ai oublié le nom d'utilisateur et le mot de passe d'administration iDRAC.	Vous devez rétablir les paramètres par défaut d'iDRAC. 1. Redémarrez le serveur et appuyez sur <Ctrl><E> lorsque le système vous y invite afin d'entrer dans l'utilitaire de configuration iDRAC. 2. Dans le menu de l'utilitaire de configuration, mettez en surbrillance **Restaurer les paramètres par défaut** et appuyez sur <Entrée>. Pour plus d'informations, voir Rétablir les paramètres par défaut.
Comment puis-je changer le nom du logement de mon serveur ?	1. Connectez-vous à l'interface Web CMC. 2. Ouvrez l'arborescence du **châssis** et cliquez sur **Serveurs**. 3. Cliquez sur l'onglet **Configuration**. 4. Tapez le nouveau nom du logement dans la ligne correspondant à votre serveur. 5. Cliquez sur **Appliquer**.
Lors du démarrage d'une session de redirection de console à partir de l'interface Web iDRAC, un message contextuel de sécurité ActiveX apparaît.	iDRAC n'est peut-être pas un site sécurisé du navigateur client. Pour empêcher l'affichage du message contextuel de sécurité à chaque démarrage d'une session de redirection de console, ajoutez iDRAC à la liste des sites sécurisés : 1. Cliquez sur **Outils**→ **Options Internet...**→ **Sécurité**→ **Sites sécurisés**. 2. Cliquez sur **Sites** et entrez l'adresse IP ou le nom DNS d'iDRAC. 3. Cliquez sur **Ajouter**.
Lorsque je démarre une session de redirection de console, l'écran du visualiseur est vierge.	Si vous disposez du privilège **Média virtuel** mais non pas du privilège **Redirection de console**, vous êtes en mesure de démarrer le visualiseur afin de pouvoir accéder à la fonctionnalité de média virtuel. Toutefois, la console du serveur géré ne s'affichera pas.
iDRAC ne démarre pas.	Retirez et réinsérez le serveur. Allez dans l'interface Web CMC afin de déterminer si iDRAC apparaît en tant que composant pouvant être mis à niveau. S'il apparaît, suivez les instructions de la section Récupération du micrologiciel iDRAC à l'aide de CMC.

	Si vous n'arrivez pas à corriger le problème, contactez le support technique.
Lors de la tentative de démarrage du serveur géré, le voyant d'alimentation est vert, mais aucun POST ou aucune vidéo ne s'affiche.	Cela peut se produire si l'une des conditions suivantes est réunie : • La mémoire n'est pas installée ou est inaccessible. • L'UC n'est pas installée ou est inaccessible. • La carte adaptatrice de connexion vidéo est manquante ou incorrectement connectée. En outre, recherchez les messages d'erreur dans le journal iDRAC à partir de l'interface Web iDRAC ou de l'écran LCD.

Retour à la page du sommaire

Retour à la page du sommaire

Glossaire

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 RSC, elle la contrôle et vérifie les informations qu'elle contient. Si le postulant remplit les normes de sécurité de l'autorité de certification, cette dernière lui envoie un certificat 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.

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).

CMC

Abréviation de Enclosure Management Controller (contrôleur de gestion de l'enceinte), l'interface de contrôleur entre iDRAC et le contrôleur CMC du système géré.

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. iDRAC 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).

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.

iAMT

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

ICMB

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

ICMP

Abréviation 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 (référence utilisateur) ou l'identificateur d'objet (numéro d'objet).

iDRAC

Abréviation de Dell Remote Access Controller 5.

iDRAC

Sigle d'Integrated Dell Remote Access Controller, le système de contrôle/surveillance « Système sur une puce » intégré des serveurs Dell 10G PowerEdge.

interruption SNMP

Une notification (événement) générée par le contrôleur iDRAC ou CMC qui contient des informations sur les changements d'état du serveur 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 iDRAC et le contrôleur CMC.

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).

MII

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).

OSCAR

Sigle de On Screen Configuration and Reporting (configuration et génération de rapports à l'écran). OSCAR est le menu affiché par iKVM d'Avocent lorsque vous appuyez sur <Impr. écran>. Il vous permet de sélectionner la console CMC ou la console iDRAC d'un serveur installé dans CMC.

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 iDRAC.

redirection de console

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

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.

RSC

Abréviation de requête de signature de certificat.

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 à iDRAC ; elle utilise des objets Active Directory définis par Dell.

schéma standard

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

SEL

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

serveur géré

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

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).

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 à iDRAC à distance.

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