Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Remarques et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données en cas de non-respect des instructions.

Mars 2009 Rév. A00

Retour à la page du sommaire

Présentation de la sous-commande RACADM

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

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

---

help

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

Tableau A-1. Commande help

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

Synopsis

```
racadm help

racadm help <sous-commande>
```

Description

La sous-commande **help** répertorie toutes les sous-commandes disponibles avec la commande **racadm,** avec une ligne de description. Vous pouvez aussi entrer 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

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

Tableau A-2. config/getconfig

Sous-commande	Définition
config	Permet de configurer iDRAC6.
getconfig	Permet d'obtenir les données de configuration iDRAC6.

Synopsis

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

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

Interfaces prises en charge

- RACADM locale

Description

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

Entrée

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 iDRAC6. Le fichier doit contenir des données au 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**. La valeur <*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, et 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 iDRAC6. 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 ou index non valide, ou autres éléments non valides de la base de données
- Échecs de la CLI RACADM

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

Exemples

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

  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`

  Permet de configurer ou de reconfigurer iDRAC6. 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 iDRAC6 un par un ou bien de récupérer et d'enregistrer dans un fichier l'ensemble des groupes de configuration iDRAC6.

Entrée

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 iDRAC6 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** dans le fichier.
-g	L'option de groupe **-g** <*nom du groupe*> permet d'afficher la configuration d'un groupe unique. Le *nom du groupe* est le nom du groupe utilisé dans les fichiers **racadm.cf**g. Si le groupe est indexé, l'option **-i** doit être utilisée.
-h	L'option d'aide **-h** affiche la liste de tous les groupes de configuration disponibles que vous pouvez utiliser. Cette option est utile si vous ne vous souvenez plus des noms exacts des groupes.
-i	L'option d'index, **-i** <*index*>, n'est 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, et 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 valides, ou d'autres éléments non valides de la base de données
- Échecs de transport de l'interface de ligne de commande RACADM

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

Exemples

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig –f myrac.cfg`

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

- `racadm getconfig -h`

  Affiche une liste des groupes de configuration disponibles sur iDRAC6.

- `racadm getconfig -u root`

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

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

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

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 de session du gestionnaire de session.

Synopsis

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

Description

La commande **getssninfo** renvoie la liste des utilisateurs connectés à iDRAC6. 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

Entrée

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`

Tableau A-7 fournit un exemple de sortie de la commande **racadm getssninfo**.

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

Utilisateur	Adresse IP	Type	Consoles
root	192.168.0.10	Telnet	KVM virtuel

- racadm getssninfo -A

  root" 143.166.174.19 "Telnet" "AUCUN"

- racadm getssninfo -A -u *

  root" 143.166.174.19 "Telnet" "AUCUN"

- bob" "143.166.174.19" "GUI" "AUCUN"

---

getsysinfo

Tableau A-8 décrit la sous-commande **racadm getsysinfo**.

Tableau A-8. getsysinfo

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

Synopsis

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

Description

La sous-commande **getsysinfo** affiche des informations relatives à iDRAC6, au serveur géré et à la configuration de surveillance.

Interfaces prises en charge

- RACADM locale

Entrée

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 iDRAC6.
-s	Affiche les informations sur le système
w	Affiche les informations sur la surveillance
-A	Élimine l'impression des en-têtes/noms.

Résultat

La sous-commande **getsysinfo** affiche des informations relatives à iDRAC6, au serveur géré et à la configuration de surveillance.

Exemple de sortie

```
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 **Hostname** et **OS Name** 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

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 la date au format *aaaammjjhhmmss.mmmmmms*, qui correspond au même format que celui renvoyé par la commande **date** d'UNIX®.

Résultat

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

Exemple de sortie

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

Interfaces prises en charge

- RACADM locale

---

setniccfg

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 iDRAC6.

- L'option **-d** active le protocole DHCP pour le NIC (la valeur par défaut est DHCP activé).
- L'option **-s** active les paramètres IP statiques. L'adresse IP, le masque de réseau et la passerelle peuvent être spécifiés. Sinon, les paramètres statiques existants sont utilisés. Les valeurs <*adresse IP*>, <*masque de réseau*> et <*passerelle*> doivent être entrées 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. Les valeurs <*adresse IP*>, <*masque de réseau*> et <*passerelle*> doivent être entrées 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

Tableau A-12 décrit la sous-commande **getniccfg**.

Tableau A-12. getniccfg

Sous-commande	Définition
getniccfg	Affiche la configuration IP actuelle d'iDRAC6.

Synopsis

```
racadm getniccfg
```

Description

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

Exemple de sortie

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

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Interfaces prises en charge

- RACADM locale

---

getsvctag

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

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

```
Y76TP0G
```

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

Interfaces prises en charge

- RACADM locale

---

racreset

Tableau A-14 décrit la sous-commande **racreset**.

Tableau A-14. racreset

Sous-commande	Définition
racreset	Réinitialise iDRAC6.

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

Synopsis

```
racadm racreset
```

Description

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

Exemples

- `racadm racreset`

  Démarre la séquence de réintialisation logicielle d'iDRAC6.

Interfaces prises en charge

- RACADM locale

---

racresetcfg

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 du 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 servant à restaurer les paramètres par défaut d'iDRAC6.

REMARQUE : Cette commande supprime votre configuration iDRAC6 actuelle et réinitialise les paramètres par défaut d'iDRAC6. 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

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. Tableau A-17 décrit les options de contrôle de l'alimentation **serveraction**.

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

Chaîne	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 mettre hors tension puis sous tension le système. - **powerstatus** : affiche l'état actuel de l'alimentation du serveur (**Activé** ou **Désactivé**). - **hardreset** : effectue une opération de réinitialisation (redémarrage) sur le 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

Tableau A-18 décrit la commande **racadm getraclog**.

Tableau A-18. getraclog

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

Synopsis

```
racadm getraclog -i

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

Description

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

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 la sortie sans en-tête ou nom.
-c	Fournit le nombre maximum d'entrées à renvoyer.
-m	Affiche un écran d'informations à la fois et invite l'utilisateur à continuer (semblable à la commande **more** 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 de la sortie indique le numéro d'enregistrement, l'horodatage, la source et la description. L'horodatage commence à minuit, le 1er janvier et augmente jusqu'à ce que le serveur géré redémarre. Après le démarrage du serveur géré, l'heure système du serveur géré est utilisée pour l'horodatage.

Exemple de sortie

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

Interfaces prises en charge

- RACADM locale

---

clrraclog

Synopsis

```
racadm clrraclog
```

Description

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

---

getsel

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 du journal SEL.

Synopsis

```
racadm getsel -i

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

Description

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

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

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

Par exemple :

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

Interfaces prises en charge

- RACADM locale

---

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

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 nombre] [-s démarrer l'enregistrement] [-m]
```

Description

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

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** d'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 par défaut de la sortie indique le numéro d'enregistrement, l'horodatage, la source et la description. L'horodatage commence à minuit, le 1er janvier et augmente jusqu'à ce que le système 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

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 (CSR) SSL à partir du RAC.

Synopsis

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

racadm sslcsrgen -s
```

Description

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

Options

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

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

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

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

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

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

Exemples

```
racadm sslcsrgen -s

ou

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

Interfaces prises en charge

- RACADM locale

---

sslcertupload

Tableau A-26 décrit la sous-commande **sslcertupload**.

Tableau A-26. sslcertupload

Sous-commande	Description
sslcertupload	Télécharge un serveur SSL personnalisé ou un certificat CA depuis le client vers iDRAC6.

Synopsis

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

Options

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 télécharger, soit le certificat CA, soit le certificat du serveur. 1 = certificat du serveur 2 = certificat CA
-f	Spécifie le nom de fichier du certificat à télécharger. Si le fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.

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

Exemple

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

Interfaces prises en charge

- RACADM locale

---

sslcertdownload

Tableau A-28 décrit la sous-commande **sslcertdownload**.

Tableau A-28. sslcertdownload

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

Synopsis

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

Options

Tableau A-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 télécharger. Si l'option **-f** ou le nom de fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.

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

Exemple

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

Interfaces prises en charge

- RACADM locale

---

sslcertview

Tableau A-30 décrit la sous-commande **sslcertview**.

Tableau A-30. sslcertview

Sous-commande	Description
sslcertview	Affiche le serveur SSL ou le certificat CA existant sur iDRAC6.

Synopsis

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

Options

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 sortie

```
racadm sslcertview -t 1

Serial Number            : 00
```

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

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 d'iDRAC6.

Synopsis

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

Description

Envoie un e-mail test depuis iDRAC6 vers une destination spécifiée.

Avant d'exécuter la commande testemail, assurez-vous que l'index spécifié dans le groupe **cfgEmailAlert** RACADM est activé et configuré correctement. 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 user1@mycompany.com
Définir le message personnalisé qui est envoyé à l'adresse e-mail de destination	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!" (« C'est un test ! »)

Vérifier si l'adresse IP SNMP est configurée correctement	racadm config -g cfgRemoteHosts -o 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

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

Aucune.

Interfaces prises en charge

- RACADM locale

---

testtrap

Tableau A-35 décrit la sous-commande **testtrap**.

Tableau A-35. testtrap

Sous-commande	Description
testtrap	Teste la fonctionnalité d'alerte par interruption SNMP iDRAC6.

Synopsis

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

Description

La sous-commande **testtrap** teste la fonctionnalité d'alerte par interruption SNMP iDRAC6 en envoyant une interruption test depuis iDRAC6 vers un écouteur cible spécifié sur le réseau.

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

Tableau A-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

Entrée

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

Synopsis

```
racadm vmdisconnect
```

Description

La sous-commande **vmdisconnect** permet de stopper toute connexion au média virtuel.

---

clrasrscreen

Synopsis

```
racadm clrasrscreen
```

Description

Efface l'écran de la dernière panne (ASR).

---

localconredirdisable

Synopsis

```
racadm localconredirdisable [0, 1]
```

Description

Désactive le kVM local depuis le système local.

Valeurs valides

`0` = Activer

`1` = Désactiver

---

vmkey

Synopsis

```
racadm vmkey [ reset ]
```

Description

La sous-commande **vmkey** permet de réinitialiser la clé du média virtuel sur sa taille initiale de 256 Mo.

Valeurs valides

`reset` = Restaure la valeur par défaut de la clé (256 Mo)

---

version

Synopsis

```
racadm version
```

Description

Affiche la version RACADM.

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 iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

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

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

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

Caractères affichables

Les caractères affichables comprennent le jeu suivant :

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

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

Description

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

idRacBuildInfo (lecture seule)

Valeurs valides

Chaîne de 16 caractères ASCII au maximum.

Valeur par défaut

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

Description

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

idRacName (lecture seule)

Valeurs valides

Chaîne de 15 caractères ASCII au maximum.

Valeur par défaut

iDRAC

Description

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

idRacType (lecture seule)

Valeurs valides

ID de produit

Valeur par défaut

8

Description

Identifie le type de Remote Access Controller comme étant CMC.

---

cfgOobSnmp

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

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

cfgOobSnmpAgentCommunity (lecture/écriture)

Valeurs valides

Chaîne de caractères. Longueur maximale = 31.

Valeur par défaut

public

Description

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

cfgOobSnmpAgentEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive l'agent SNMP dans le RAC.

---

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 actives utilisateur ; les utilisateurs devront se reconnecter en utilisant les nouveaux paramètres de l'adresse IP.

cfgDNSDomainNameFromDHCP (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

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 un des caractères doit être alphabétique. Seuls les caractères alphanumériques, les tirets et les points sont valides.

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

Valeur par défaut

(vide)

Description

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

cfgDNSRacName (lecture/écriture)

Valeurs valides

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

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

Valeur par défaut

idrac-*numéro de service*

Description

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

cfgDNSRegisterRac (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Enregistre le nom iDRAC6 sur le serveur DNS.

cfgDNSServersFromDHCP (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgDNSServer1 (lecture/écriture)

Valeurs valides

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

Valeur par défaut

0.0.0.0

Description

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

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

cfgDNSServer2 (lecture/écriture)

Valeurs valides

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

Valeur par défaut

0.0.0.0

Description

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

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

cfgNicEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive le contrôleur d'interface réseau iDRAC. Si le NIC est désactivé, les interfaces réseau distantes d'iDRAC6 ne sont plus accessibles et iDRAC6 est seulement disponible via l'interface RACADM locale.

cfgNicIpAddress (lecture/écriture)

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

Valeurs valides

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

Valeur par défaut

192.168.0.*n*

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

Description

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

cfgNicNetmask (lecture/écriture)

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

Valeurs valides

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

Valeur par défaut

255.255.255.0

Description

Masque de sous-réseau utilisé pour l'attribution statique de l'adresse IP d'iDRAC6. Cette propriété n'est valide que si **cfgNicUseDhcp** est défini sur **0** (FAUX).

cfgNicGateway (lecture/écriture)

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

Valeurs valides

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

Valeur par défaut

192.168.0.1

Description

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

cfgNicUseDhcp (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Spécifie si le DHCP est utilisé pour attribuer l'adresse IP iDRAC6. Si cette propriété est définie sur 1 (TRUE), l'adresse IP iDRAC6, le masque de sous-réseau et la passerelle sont attribués à partir du serveur DHCP sur le réseau. Si cette propriété est définie sur **0** (FALSE), l'adresse IP statique, le masque de sous-réseau et la passerelle sont attribués à partir des propriétés **cfgNicIpAddress**, **cfgNicNetmask** et **cfgNicGateway**.

cfgNicMacAddress (lecture seule)

Valeurs valides

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

Valeur par défaut

Adresse MAC actuelle du NIC iDRAC6. Par exemple, 00:12:67:52:51:A3.

Description

Adresse MAC du NIC iDRAC6.

---

cfgUserAdmin

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

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

cfgUserAdminIndex (lecture seule)

Valeurs valides

Ce paramètre est renseigné en fonction des instances existantes.

Valeur par défaut

1 - 16

Description

L'index unique d'un utilisateur.

cfgUserAdminIpmiLanPrivilege (lecture/écriture)

Valeurs valides

2 (**utilisateur**)

3 (opérateur)

4 (**administrateur**)

15 (**pas d'accès**)

Valeur par défaut

4 (utilisateur 2)

15 (tous les autres)

Description

Privilège maximum sur le canal LAN IPMI.

cfgUserAdminPrivilege (lecture/écriture)

Valeurs valides

0x00000000 à 0x000001ff, et 0x0

Valeur par défaut

0x00000000

Description

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

Tableau B-1. Masques binaires pour les privilèges utilisateur

Privilège utilisateur	Masque binaire de privilège
Ouvrir une session iDRAC6	0x0000001
Configurer un serveur iDRAC6	0x0000002
Configurer les utilisateurs	0x0000004
Effacer les journaux	0x0000008
Exécuter les commandes de contrôle du serveur	0x0000010
Accéder à la redirection de console	0x0000020
Accéder au média virtuel	0x0000040
Tester les alertes	0x0000080
Exécuter les commandes de débogage	0x0000100

Exemples

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

Tableau B-2. Exemple de masques binaires pour les privilèges utilisateur

Privilège(s) utilisateur	Masque binaire de privilège
L'utilisateur n'est pas autorisé à accéder à iDRAC6.	0x00000000
L'utilisateur peut uniquement se connecter à iDRAC6 et afficher les informations de configuration d'iDRAC6 et du serveur.	0x00000001
L'utilisateur peut se connecter iDRAC6 et modifier la configuration.	0x00000001 + 0x00000002 = 0x00000003
L'utilisateur peut ouvrir une session sur le RAC, accéder au média virtuel et à la redirection de console.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lecture/écriture)

Valeurs valides

Chaîne de caractères. Longueur maximale = 16

Valeur par défaut

(vide)

Description

Le nom d'utilisateur pour cet index. L'index utilisateur est créé en écrivant une chaîne de caractères dans ce champ de nom si l'index est vide. L'écriture d'une chaîne de guillemets anglais ("") supprime l'utilisateur qui correspond à cet index. Vous ne pouvez pas modifier le nom. Vous devez supprimer puis recréer le nom. La chaîne 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

(vide)

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 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive un utilisateur.

cfgUserAdminSolEnable

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

---

cfgEmailAlert

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

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

cfgEmailAlertIndex (lecture seule)

Valeurs valides

1-4

Valeur par défaut

Ce paramètre est renseigné en fonction des instances existantes.

Description

Index unique d'une instance d'alerte.

cfgEmailAlertEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgEmailAlertAddress

Valeurs valides

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

Valeur par défaut

(vide)

Description

Adresse e-mail de la source d'alertes.

cfgEmailAlertCustomMsg

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

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

cfgSessionManagement

Ce groupe contient les paramètres pour configurer le nombre de sessions qui peuvent se connecter à iDRAC6.

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

cfgSsnMgtConsRedirMaxSessions (lecture/écriture)

Valeurs valides

1 - 4

Valeur par défaut

4

Description

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

cfgSsnMgtWebserverTimeout (lecture/écriture)

Valeurs valides

60 - 10800

Valeur par défaut

1800

Description

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

Une session de serveur Web expirée ferme la session actuelle.

cfgSsnMgtSshIdleTimeout (lecture/écriture)

Valeurs valides

0 (pas de délai d'attente)

60 - 10800

Valeur par défaut

1800

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

Une session Secure Shell 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 - 10800

Valeur par défaut

1800

Description

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

Une session Telnet expirée affiche le message d'erreur suivant 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 iDRAC6.

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

cfgSerialSshEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

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

cfgSerialTelnetEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

---

cfgRemoteHosts

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

cfgRhostsSmtpServerIpAddr (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une adresse IP valide du serveur SMTP. Par exemple : 192.168.0.56.

Valeur par défaut

0.0.0.0

Description

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

---

cfgUserDomain

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

cfgUserDomainIndex (lecture seule)

Valeurs valides

1 - 40

Valeur par défaut

<instance>

Description

Représente un domaine spécifique

cfgUserDomainName (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères au maximum.

Valeur par défaut

(vide)

Description

Spécifie le nom de domaine utilisateur Active Directory

---

cfgServerPower

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

cfgServerPowerStatus (lecture seule)

Valeurs valides

1 = TRUE

0 = FALSE

Valeur par défaut

0

Description

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

cfgServerPowerServerAllocation (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Représente le bloc d'alimentation disponible pour le serveur

cfgServerPowerActualPowerConsumption (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Représente la consommation électrique actuelle du serveur

cfgServerPowerPeakPowerConsumption (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Représente la consommation électrique maximale du serveur jusqu'à présent

cfgServerPowerPeakPowerTimestamp (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Heure à laquelle le pic de consommation électrique a été enregistré

cfgServerPowerConsumptionClear (lecture seule)

Valeurs valides

0, 1

Valeur par défaut

0

Description

Réinitialise la propriété **cfgServerPeakPowerConsumption** sur 0 et la propriété **cfgServerPeakPowerConsumptionTimestamp** est établie sur la configuration temporelle iDRAC6

cfgServerPowerCapWatts (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Représente le seuil d'alimentation du serveur en Watts

cfgServerPowerCapBtuhr (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Représente le seuil d'alimentation du serveur en BTU/h

cfgServerPowerCapPercent (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

(vide)

Description

Représente le seuil d'alimentation du serveur en pourcentage

---

cfgRacTuning

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

cfgRacTuneHttpPort (lecture/écriture)

Valeurs valides

10 - 65 535

Valeur par défaut

80

Description

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

cfgRacTuneHttpsPort (lecture/écriture)

Valeurs valides

10 - 65 535

Valeur par défaut

443

Description

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

cfgRacTuneIpRangeEnable

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de validation de la plage d'adresses IP iDRAC6

cfgRacTuneIpRangeAddr

Valeurs valides

Une chaîne au format adresse IP. Par exemple, 192.168.0.44.

Valeur par défaut

192.168.1.1

Description

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

cfgRacTuneIpRangeMask

Valeurs valides

Valeurs de masque IP standard avec bits justifiés à gauche

Valeur par défaut

255.255.255.0

Description

Une chaîne au format adresse IP. Par exemple, 255.255.255.0.

cfgRacTuneIpBlkEnable

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité Blocage de l'adresse IP du 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 - 65 535

Valeur par défaut

60

Description

Définit la période en secondes pendant laquelle les tentatives échouées sont comptées. Lorsque le nombre d'échecs dépasse cette limite, les échecs ne sont plus comptabilisés.

cfgRacTuneIpBlkPenaltyTime

Valeurs valides

10 - 65 535

Valeur par défaut

300

Description

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

cfgRacTuneSshPort (lecture/écriture)

Valeurs valides

1 - 65 535

Valeur par défaut

22

Description

Spécifie le numéro de port utilisé pour l'interface SSH iDRAC6

cfgRacTuneConRedirEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

Active ou désactive la redirection de console

cfgRacTuneTelnetPort (lecture/écriture)

Valeurs valides

1 - 65 535

Valeur par défaut

23

Description

Spécifie le numéro de port utilisé pour l'interface Telnet iDRAC6

cfgRacTuneConRedirEncryptEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

Crypte la vidéo dans une session de redirection de console

cfgRacTuneConRedirPort (lecture/écriture)

Valeurs valides

1 - 65 535

Valeur par défaut

5900

Description

Spécifie le port utilisé pour le clavier et la souris pendant l'activité de redirection de console avec iDRAC6

cfgRacTuneConRedirVideoPort (lecture/écriture)

Valeurs valides

1 - 65 535

Valeur par défaut

5901

Description

Spécifie le port utilisé pour la vidéo pendant l'activité de redirection de console avec iDRAC6

REMARQUE : Cet objet nécessite une réinitialisation d'iDRAC6 pour devenir actif.

cfgRacTuneAsrEnable (lecture/écriture)

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

REMARQUE : Cet objet nécessite une réinitialisation d'iDRAC6 pour devenir actif.

cfgRacTuneWebserverEnable (lecture/écriture)

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active et désactive le serveur Web iDRAC6 Si cette propriété est désactivée, iDRAC6 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 (met en marche) ou désactive (éteint) la vidéo du serveur local

cfgRacTuneLocalConfigDisable (lecture/écriture)

Valeurs valides

0 (active)

1 (désactive)

Valeur par défaut

0

Description

Désactive l'accès en écriture aux données de configuration iDRAC6 L'accès est activé par défaut.

REMARQUE : L'accès peut être désactivé à l'aide de l'interface RACADM locale ou de l'interface Web iDRAC6 ; toutefois, une fois désactivé, l'accès peut uniquement être réactivé via l'interface Web iDRAC6.

---

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (lecture seule)

Valeurs valides

Chaîne de 255 caractères au maximum.

Valeur par défaut

(vide)

Description

Nom d'hôte du serveur géré

ifcRacMnOsOsName (lecture seule)

Valeurs valides

Chaîne de 255 caractères au maximum.

Valeur par défaut

(vide)

Description

Nom du système d'exploitation du serveur géré

---

cfgRacSecurity

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

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

cfgSecCsrCommonName (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

Description

Spécifie le nom commun (CN) de la RSC

cfgSecCsrOrganizationName (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

(vide)

Description

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

cfgSecCsrOrganizationUnit (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

(vide)

Description

Spécifie le service de l'organisation (OU) pour la RSC

cfgSecCsrLocalityName (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

(vide)

Description

Spécifie la ville (L) pour la RSC

cfgSecCsrStateName (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

(vide)

Description

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

cfgSecCsrCountryCode (lecture/écriture)

Valeurs valides

Chaîne de deux caractères.

Valeur par défaut

(vide)

Description

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

cfgSecCsrEmailAddr (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

(vide)

Description

Spécifie l'adresse e-mail de la RSC.

cfgSecCsrKeySize (lecture/écriture)

Valeurs valides

512

1024

2048

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 iDRAC6. Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

cfgVirMediaAttached (lecture/écriture)

Valeurs valides

0 = Déconnecter

1 = Connecter

2 = Autoconnecter

Valeur par défaut

0

Description

Cet objet est utilisé pour connecter les périphériques virtuels au système via le bus USB. Lorsque les périphériques sont reliés, le serveur reconnaît les périphériques de stockage de masse USB valides reliés au système. Cela revient à relier un lecteur de CD-ROM/disquette USB local à un port USB sur le système. Lorsque les périphériques sont reliés, vous pouvez alors vous connecter aux périphériques virtuels à distance à l'aide de l'interface Web iDRAC6 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.

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 iDRAC6. 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.

cfgVirMediaKeyEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de clé du média virtuel d'iDRAC6

cfgFloppyEmulation (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

---

cfgActiveDirectory

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité Active Directory iDRAC6.

cfgADRacDomain (lecture/écriture)

Valeurs valides

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

Valeur par défaut

(vide)

Description

Domaine Active Directory où se trouve le DRAC

cfgADRacName (lecture/écriture)

Valeurs valides

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

Valeur par défaut

(vide)

Description

Nom de l'iDRAC6 enregistré dans la forêt Active Directory

cfgADEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgADAuthTimeout (lecture/écriture)

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

cfgADDomainController1 (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADDomainController2 (lecture/écriture)

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADDomainController3 (lecture/écriture)

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADGlobalCatalog1 (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADGlobalCatalog2 (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

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

cfgADGlobalCatalog3 (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet

Valeur par défaut

Aucune valeur par défaut

Description

iDRAC6 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

Description

Détermine le type de schéma à utiliser avec Active Directory

cfgADCertValidationEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

Active ou désactive la validation de certificat 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

1 - 5

Description

Index du groupe de rôles tel qu'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

(vide)

Description

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

cfgSSADRoleGroupDomain (lecture/écriture)

Valeurs valides

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

Valeur par défaut

(vide)

Description

Domaine Active Directory où se trouve le groupe de rôles

cfgSSADRoleGroupPrivilege (lecture/écriture)

Valeurs valides

0x00000000 à **0x000001ff**

Valeur par défaut

(vide)

Description

Utilisez les nombres de masque binaire dans Tableau B-3 pour définir les privilèges d'autorité basés sur les rôles pour un groupe de rôles.

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

Privilège Groupe de rôles	Masque binaire
Ouvrir une session iDRAC6	0x00000001
Configurer un serveur iDRAC6	0x00000002
Configurer les utilisateurs	0x00000004
Effacer les journaux	0x00000008
Exécuter les commandes de contrôle du serveur	0x00000010
Accéder à la redirection de console	0x00000020
Accéder au média virtuel	0x00000040
Tester les alertes	0x00000080
Exécuter les commandes de débogage	0x00000100

---

cfgIpmiSol

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

cfgIpmiSolEnable (lecture/écriture)

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive les communications série sur le réseau local

cfgIpmiSolBaudRate (lecture/écriture)

Valeurs valides

9600, 19200, 57600, 115200

Valeur par défaut

115200

Description

Débit en bauds pour la communication série sur le réseau local

cfgIpmiSolMinPrivilege (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

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

cfgIpmiSolAccumulateInterval (lecture/écriture)

Valeurs valides

1 - 255

Valeur par défaut

10

Description

Spécifie le temps d'attente type d'iDRAC6 avant la transmission d'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 (FALSE)

1 (TRUE)

Valeur par défaut

0

Description

Active ou désactive l'interface IPMI sur le réseau local

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 réseau local

cfgIpmiLanAlertEnable (lecture/écriture)

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

0

Description

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

cfgIpmiEncryptionKey (lecture/écriture)

Valeurs valides

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

Valeur par défaut

00000000000000000000000000000000000000000

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 plate-forme disponibles sur le serveur géré.

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

cfgIpmiPefName (lecture seule)

Valeurs valides

Chaîne de 255 caractères au maximum.

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 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

---

cfgIpmiPet

Ce groupe est utilisé pour configurer des interruptions d'événements sur 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 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive une interruption spécifique

Retour à la page du sommaire

Retour à la page du sommaire

Base de données des propriétés SM-CLP iDRAC6

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

---

/system1/sp1/account<1-16>

Cette cible fournit des informations de configuration sur les utilisateurs locaux qui ont le droit d'accéder au RAC via les interfaces distantes disponibles. Jusqu'à 16 instances du groupe d'utilisateurs sont autorisées. Chaque instance <1-16> représente la configuration d'un utilisateur local individuel.

userid (lecture seule)

Valeurs valides

1-16

Valeur par défaut

Dépend de l'instance du compte actuellement accédée.

Description

Spécifie l'ID de l'instance ou l'ID de l'utilisateur local.

username (lecture/écriture)

Valeurs valides

Chaîne de caractères. Longueur maximale = 16

Valeur par défaut

""

Description

Chaîne de texte contenant le nom de l'utilisateur local de ce compte. La chaîne ne doit pas contenir de barre oblique (/), de point (.), de symbole « chez » (@) ou de guillemets ("). Pour supprimer l'utilisateur, supprimez le compte. (supprimer le compte<1-16>).

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

oemdell_ipmilanprivileges (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.

password (écriture seule)

Valeurs valides

Chaîne de texte comprise entre 4 et 20 caractères.

Valeur par défaut

""

Description

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

enabledstate (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

Permet d'activer ou de désactiver un utilisateur individuel.

solenabled (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

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

oemdell_extendedprivileges (lecture/écriture)

Valeurs valides

0x00000000 à 0x000001ff

Valeur par défaut

0x00000000

Description

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

Tableau C-1. Masques binaires pour les privilèges utilisateur

Privilège utilisateur	Masque binaire de privilège
Ouvrir une session sur iDRAC6	0x0000001
Configurer iDRAC6	0x0000002
Configurer les utilisateurs	0x0000004
Effacer les journaux	0x0000008
Exécuter les commandes de contrôle du serveur	0x0000010
Accéder à la redirection de console	0x0000020
Accéder au média virtuel	0x0000040
Tester les alertes	0x0000080
Exécuter les commandes de débogage	0x0000100

Exemples

Tableau C-2 fournit des exemples de masques binaires de privilèges pour les utilisateurs avec un ou plusieurs privilèges.

Tableau C-2. Exemple de masques binaires pour les privilèges utilisateur

Privilège(s) utilisateur	Masque binaire de privilège
L'utilisateur n'est pas autorisé à accéder à iDRAC6.	0x00000000
L'utilisateur peut uniquement ouvrir une session sur iDRAC6 et afficher les informations de configuration d'iDRAC6 et du serveur.	0x00000001
L'utilisateur peut ouvrir une session sur iDRAC6 et modifier la configuration.	0x00000001 + 0x00000002 = 0x00000003
L'utilisateur peut ouvrir une session sur le RAC, accéder au média virtuel et à la redirection de console.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

/system1/sp1/enetport1/*

Ce groupe contient les paramètres qui permettent de configurer le NIC d'iDRAC6. Une seule instance du groupe est autorisée. Tous les objets de ce groupe nécessitent une réinitialisation du NIC d'iDRAC6, ce qui interrompra peut-être brièvement la connectivité. Les objets qui modifient les paramètres de l'adresse IP du NIC d'iDRAC6 entraîneront la fermeture de toutes les sessions utilisateur actives et obligeront les utilisateurs à se reconnecter en utilisant les paramètres mis à jour de l'adresse IP.

macaddress (lecture seule)

Valeurs valides

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

Valeur par défaut

Adresse MAC actuelle du NIC d'iDRAC6. Par exemple, 00:12:67:52:51:A3.

Description

Détient l'adresse MAC du NIC d'iDRAC6.

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_nicenable (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

Active ou désactive le NIC d'iDRAC6. Si le NIC est désactivé, les interfaces réseau distantes vers iDRAC6 deviennent inaccessibles, rendant iDRAC6 disponible uniquement via l'interface RACADM locale.

ipaddress (lecture/écriture)

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 égal à 120 plus le numéro de logement du serveur)

Description

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

subnetmask (lecture/écriture)

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 iDRAC6. Cette propriété n'est valide que si oemdell_usedhcp est défini sur 0 (désactivé).

oemdell_usedhcp (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

Spécifie si le DHCP est utilisé pour attribuer l'adresse IP iDRAC6. Si cette propriété est définie sur 1 (activé), l'adresse IP iDRAC6, 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 (désactivé), l'adresse IP statique, le masque de sous-réseau et la passerelle obtiennent des valeurs insérées manuellement par l'utilisateur.

committed (lecture/écriture)

Valeurs valides

0 (en attente d'engagement)

1 (engagé)

Valeur par défaut

1

Description

Permet à l'utilisateur de changer l'adresse IP et/ou le masque de sous-réseau sans mettre fin à la session en cours. Si cette propriété est définie sur 1 (engagé), l'adresse IP et le masque de sous-réseau sont valides. Toute modification de l'adresse IP ou du masque de sous-réseau convertit automatiquement cette propriété sur 0 (en attente d'engagement). Pour que les paramètres réseau soient effectifs, la propriété doit être redéfinie sur 1.

/system1/sp1/enetport1/lanendpt1/ipendpt1/ dnsendpt1

oemdell_domainnamefromdhcp (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

Spécifie que le nom de domaine DNS iDRAC6 doit être attribué à partir du serveur DHCP réseau.

oemdell_dnsdomainname (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères ASCII au maximum. Au moins un des caractères doit être alphabétique.

Valeur par défaut

""

Description

Détient le nom de domaine DNS. Ce paramètre n'est valide que si oemdell_domainnamefromdhcp est défini sur 0 (désactivé).

oemdell_dnsregisterrac (lecture/écriture)

Valeurs valides

0 (non enregistré)

1 (enregistré)

Valeur par défaut

0

Description

Enregistre le nom d'iDRAC6 sur le serveur DNS.

oemdell_dnsracname (lecture/écriture)

Valeurs valides

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

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

Valeur par défaut

Numéro de service du RAC

Description

Affiche le nom du RAC, qui correspond au numéro de service du RAC par défaut. Ce paramètre n'est valide que si oemdell_dnsregisterrac est défini sur 1 (enregistré).

oemdell_serversfromdhcp (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

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

/system1/sp1/enetport1/lanendpt1/ipendpt1/ dnsendpt1/remotesap1

dnsserveraddress (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

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

/system1/sp1/enetport1/lanendpt1/ipendpt1/ dnsendpt1/remotesap2

dnsserveraddress (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

Spécifie l'adresse IP du serveur DNS 2. Cette propriété n'est valide que si oemdell_serversfromdhcp est défini sur 0 (désactivé).

/system1/sp1/enetport1/lanendpt1/ipendpt1/ remotesap1

defaultgatewayaddress (lecture/écriture)

Valeurs valides

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

Valeur par défaut

192.168.0.1

Description

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

/system1/sp1/groupe<1-5>

Ces groupes contiennent les paramètres qui permettent de configurer les paramètres du schéma standard d'Active Directory.

oemdell_groupname (lecture/écriture)

Valeurs valides

Toute chaîne de texte imprimable de 254 caractères maximum sans espace blanc.

Valeur par défaut

""

Description

Détient le nom du groupe de rôles tel qu'enregistré dans la forêt Active Directory.

oemdell_groupdomain (lecture/écriture)

Valeurs valides

Toute chaîne de texte imprimable de 254 caractères maximum sans espace blanc.

Valeur par défaut

""

Description

Détient le domaine Active Directory où réside le groupe de rôles.

oemdell_groupprivilege (lecture/écriture)

Valeurs valides

0x00000000 à 0x000001ff

Valeur par défaut

""

Description

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

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

Groupe de rôles	Masque binaire de privilège
Ouvrir une session sur iDRAC6	0x00000001
Configurer iDRAC6	0x00000002
Configurer les utilisateurs	0x00000004
Effacer les journaux	0x00000008
Exécuter les commandes de contrôle du serveur	0x00000010
Accéder à la redirection de console	0x00000020
Accéder au média virtuel	0x00000040
Tester les alertes	0x00000080
Exécuter les commandes de débogage	0x00000100

/system1/sp1/oemdell_adservice1

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité Active Directory iDRAC6.

enabledstate (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

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

oemdell_adracname (lecture/écriture)

Valeurs valides

Toute chaîne de texte imprimable de 254 caractères maximum sans espace blanc.

Valeur par défaut

""

Description

Nom d'iDRAC6 enregistré dans la forêt Active Directory.

oemdell_adracdomain (lecture/écriture)

Valeurs valides

Toute chaîne de texte imprimable de 254 caractères maximum sans espace blanc.

Valeur par défaut

""

Description

Domaine Active Directory où réside iDRAC6.

oemdell_adrootdomain (lecture/écriture)

Valeurs valides

Toute chaîne de texte imprimable de 254 caractères maximum sans espace blanc.

Valeur par défaut

""

Description

Domaine racine de la forêt de domaines.

oemdell_timeout (lecture/écriture)

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.

oemdell_schematype (lecture/écriture)

Valeurs valides

1 (schéma étendu)

2 (schéma standard)

Valeur par défaut

1

Description

Détermine le type de schéma à utiliser avec Active Directory.

oemdell_adspecifyserverenable (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

Permet à l'utilisateur d'indiquer un serveur LDAP ou un serveur de catalogue global.

oemdell_addomaincontroller (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet.

Valeur par défaut

""

Description

Valeur spécifiée par l'utilisateur utilisée par iDRAC6 pour rechercher des noms d'utilisateur sur le serveur LDAP.

oemdell_adglobalcatalog (lecture/écriture)

Valeurs valides

Adresse IP valide ou nom de domaine complet.

Valeur par défaut

Aucune valeur par défaut

Description

Valeur spécifiée par l'utilisateur utilisée par iDRAC6 pour rechercher des noms d'utilisateur sur le serveur de catalogue global.

/system1/sp1/oemdell_racsecurity1

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

commonname (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

""

Description

Spécifie le nom commun de la CSR.

organizationname (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

""

Description

Spécifie le nom de compagnie de la CSR.

oemdell_organizationunit (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

""

Description

Spécifie le service de la compagnie de la CSR.

oemdell_localityname (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

""

Description

Spécifie la ville de la CSR.

oemdell_statename (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

""

Description

Spécifie le nom de l'État de la CSR.

oemdell_countrycode (lecture/écriture)

Valeurs valides

Chaîne de 2 caractères maximum.

Valeur par défaut

""

Description

Spécifie l'indicatif de pays de la CSR.

oemdell_emailaddress (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères maximum.

Valeur par défaut

""

Description

Spécifie l'adresse e-mail de la RSC.

oemdell_keysize (lecture/écriture)

Valeurs valides

1024

2048

4096

Valeur par défaut

1024

Description

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

/system1/sp1/oemdell_ssl1

Contient les paramètres nécessaires pour générer les requêtes de signature de certificat (CSR) et visualiser les certificats.

generate (lecture/écriture)

Valeurs valides

0 (ne pas générer)

1 (générer)

Valeur par défaut

0

Description

Génère une CSR lorsque la valeur est définie sur 1. Définissez les propriétés dans la cible oemdell_racsecurity1 avant de générer une CSR.

oemdell_status (lecture seule)

Valeurs valides

CSR non trouvée

CSR générée

Valeur par défaut

CSR non trouvée

Description

Affiche l'état de la précédente commande générée émise, le cas échéant, au cours de la session actuelle.

oemdell_certtype (lecture/écriture)

Valeurs valides

SSL

AD

RSC

Valeur par défaut

SSL

Description

Spécifie le type de certificat à visualiser (AD ou SSL) et permet de générer une CSR à l'aide de la propriété **generate**.

/system1/sp1/oemdell_vmservice1

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité de média virtuel iDRAC6.

enabledstate (lecture/écriture)

Valeurs valides

VMEDIA_DETACH

VMEDIA_ATTACH

VMEDIA_AUTO_ATTACH

Valeur par défaut

VMEDIA_ATTACH

Description

Permet de relier des périphériques virtuels au système via le bus USB, ce qui permet au serveur de reconnaître 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 iDRAC6 ou de la CLI. Lorsque cette propriété est définie sur 0, les périphériques ne sont plus reliés au bus USB.

oemdell_singleboot (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de démarrage unique de média virtuel d'iDRAC6. Si cette propriété est activée au réamorçage du serveur hôte, le serveur tente de s'amorcer à partir des périphériques de médias virtuels.

oemdell_floppyemulation (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

Valeur par défaut

0

Description

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

/system1/sp1/oemdell_vmservice1/tcpendpt1

portnumber (lecture/écriture)

Valeurs valides

1 - 65 535

Valeur par défaut

3668

Description

Spécifie le numéro de port utilisé pour les connexions de média virtuel cryptées vers iDRAC6.

oemdell_sslenabled (lecture seule)

Valeur légale

FALSE

Valeur par défaut

FALSE

Description

Indique que SSL est désactivé sur le port.

portnumber (lecture/écriture)

Valeurs valides

1 - 65 535

Valeur par défaut

3670

Description

Spécifie le numéro de port utilisé pour les connexions de média virtuel cryptées vers iDRAC6.

oemdell_sslenabled (lecture seule)

Valeur légale

TRUE

Valeur par défaut

TRUE

Description

Indique que SSL est activé sur le port.

Retour à la page du sommaire

Retour à la page du sommaire

Équivalences RACADM et SM-CLP

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

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

Tableau D-1. Groupes/objets RACADM et équivalences SM-CLP

Groupes/objets 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, **0** par défaut
cfgADRacName	oemdell_adracname	Chaîne de 254 caractères au maximum
cfgADRacDomain	oemdell_adracdomain	Chaîne de 254 caractères au maximum
cfgADAuthTimeout	oemdell_timeout	De 15 à 300 secondes, **120** par défaut
cfgADType	oemdell_schematype	1 pour le schéma standard, 2 pour le schéma étendu, **1** par défaut
cfgADDomainController	oemdell_addomaincontroller	Nom DNS ou adresse IP du contrôleur de domaine utilisé dans la recherche LDAP
cfgADGlobalCatalog	oemdell_adglobalcatalog	Nom DNS ou adresse IP du serveur de catalogue global utilisé dans la recherche LDAP
cfgStandardSchema		
cfgSSADRoleGroupIndex	**de /system1/sp1/group1** *à* **/system1/sp1/group5**	RACADM : ID de l'index de groupe de 1 à 5 SM-CLP : sélectionné avec le chemin de l'adresse
cfgSSADRoleGroupName	oemdell_groupname	Chaîne de 254 caractères au maximum
cfgSSADRoleGroupDomain	oemdell_groupdomain	Chaîne de 254 caractères au maximum
cfgSSADRoleGroupPrivilege	oemdell_grouppprivilege	Masque binaire avec des valeurs comprises 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 iDRAC6 par défaut : **192.168.0.120** plus le numéro de logement du serveur.
cfgNicNetmask	subnetmask	Masque de sous-réseau par défaut le réseau iDRAC6 : **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 250 caractères ASCII au maximum. Au moins un caractère doit être

		alphabétique.
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 alphabétique. Par défaut : **iDRAC-** *plus le numéro de service Dell*.
cfgDNSRegisterRac	oemdell_dnsregisterrac	À définir sur 1 pour enregistrer le nom iDRAC6 dans le DNS. Par défaut : **0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	À définir sur 1 pour obtenir les adresses de serveur DNS auprès de DHCP Par défaut : **0**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	Chaîne de caractères représentant l'adresse IP d'un serveur DNS
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap2	
cfgDNSServer2	dnsserveraddresses2	Chaîne de caractères représentant l'adresse IP d'un serveur DNS
	/system1/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	**/system1/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 le 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**.
	/system1/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**
	/system1/sp1/oemdell_vmservice1/tcpendpt2	
	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	**de /system1/sp1/account1 *à* /system1/sp1/account16**	
cfgUserAdminEnable	enabledstate	À définir sur 1 pour activer l'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 avec des valeurs comprises 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 réseau local. Par défaut : **0**
cfgUserAdminUserName	username	Chaîne de 16 caractères au maximum
cfgEmailAlert		
cfgEmailAlertAddress		Adresse e-mail de destination ; 64 caractères au maximum
cfgEmailAlertCustomMsg		Message e-mail à envoyer ; 32 caractères au maximum
cfgEmailAlertEnable		À définir sur 1 pour activer l'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 simultanées 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. De 60 à 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 iDRAC6. Par défaut : **1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		Nom d'hôte du serveur géré. Chaîne de 255 caractères au maximum
ifcRacMnOsOsName		Nom du système d'exploitation du serveur géré. Chaîne de 255 caractères au maximum
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Nom de domaine d'Active Directory. Chaîne de 254 caractères au maximum
cfgRacSecCsrCountryCode	oemdell_countrycode	Code de pays d'Active Directory. Deux caractères
cfgRacSecCsrEmailAddr	oemdell_emailaddress	Adresse e-mail à utiliser pour la requête de signature de certificat. Chaîne de 254 caractères au maximum
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 254 caractères au maximum
cfgRacSecCsrOrganizationName	organizationname	Nom de la compagnie possédant Active Directory. Chaîne de 254 caractères au maximum
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Nom du service de la compagnie possédant Active Directory. Chaîne de 254 caractères au maximum
cfgRacSecCsrStateName	oemdell_statename	Nom de l'état ou de la région où se trouve Activity Directory. Chaîne de 254 caractères au maximum
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Nombre maximal de millisecondes à attendre avant d'envoyer un paquet partiel de communications série sur le réseau local (entre 1 et 255) Par défaut : **10**

cfgIpmiSolBaudRate		Débit en bauds à utiliser pour les communications série sur le réseau local (19 200, 57 600, 115 200). Par défaut : **115 200**
cfgIpmiSolEnable		À définir sur 1 pour activer les communications série sur le réseau local. Par défaut : **0**
cfgIpmiSolSendThreshold		Nombre maximal de caractères à recueillir 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 : **0000000000000000000000000000000000000000**
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 18 caractères au maximum. 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

Tableau D-2. Sous-commandes RACADM et équivalences SM-CLP

Sous-commande RACADM	**SM-CLP**	**Description**
sslcsrgen -g	set /system1/sp1/oemdell_ssl1 oemdell_certtype=CSR set /system1/sp1/oemdell_ssl1 generate=1 dump -destination <URI TFTP de la requête de signature de certificat iDRAC> /system1/sp1/oemdell_ssl1	Génère et télécharge une requête de signature de certificat (CSR)
sslcsrgen -s	show /system1/sp1/oemdell_ssl1 oemdell_status	Renvoie la condition d'un processus de création d'une RSC
sslcertupload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <URI TFTP du certificat de serveur iDRAC> /system1/sp1/oemdell_ssl1	Télécharge le certificat de serveur iDRAC6 sur iDRAC6.
sslcertupload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <URI TFTP du certificat Active Directory> /system1/sp1/oemdell_ssl1	Transfère le certificat Active Directory sur iDRAC6.
sslcertdownload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <URI TFTP du certificat de serveur iDRAC> /system1/sp1/oemdell_ssl1	Télécharge le certificat de serveur iDRAC6 à partir d'iDRAC6.
sslcertdownload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <URI TFTP du certificat Active Directory> /system1/sp1/oemdell_ssl1	Télécharge le certificat Active Directory à partir d'iDRAC6.

Retour à la page du sommaire

Retour à la page du sommaire

Présentation d'iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

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

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

Vous pouvez configurer iDRAC6 pour qu'il vous envoie des alertes par e-mail ou d'interruption SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]) en cas d'avis ou d'erreurs. Pour vous aider à diagnostiquer la cause probable d'un plantage système, iDRAC6 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 M1000e 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. Un CMC redondant peut être ajouté pour assurer un basculement à chaud si le CMC principal échoue. Le châssis permet d'accéder aux périphériques iDRAC6 via son écran LCD, les connexions de console locale et son interface Web.

Toutes les connexions réseau à iDRAC6 s'effectuent via l'interface réseau CMC (port de connexion CMC RJ45 nommé « Gb »). CMC achemine le trafic vers les périphériques iDRAC6 sur ses serveurs par le biais d'un réseau privé interne. Ce réseau de gestion privé se trouve hors du chemin d'accès 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 iDRAC6 est désactivée par défaut. Elle doit être configurée pour pouvoir accéder à iDRAC6. Une fois iDRAC6 activé et configuré sur le réseau, il est accessible sur l'adresse IP qui lui a été attribuée via l'interface Web iDRAC6, Telnet ou SSH et les protocoles de gestion de réseau pris en charge, tels que le protocole IPMI (Interface de gestion de plateforme intelligente).

Fonctionnalités de gestion iDRAC6

iDRAC6 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 iDRAC6 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 d'événements système, au journal iDRAC6 et à l'écran du dernier plantage du système fermé subitement ou sans réponse qui est indépendant de l'état du système d'exploitation
- Intégration du logiciel Dell OpenManage™ : vous permet de lancer l'interface Web iDRAC6 à partir de Dell OpenManage Server Administrator ou d'IT Assistant
- Saisie de l'amorçage : fournit jusqu'à trois images de saisie d'amorçage en vue du débogage
- Alerte iDRAC6 : vous avertit des problèmes de nud 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
- Connexion directe depuis l'interface Web du CMC : une fois que vous êtes connecté à CMC, vous pouvez accéder à n'importe quel périphérique iDRAC6 du châssis sans avoir à vous reconnecter
- Mise à jour du micrologiciel de type un-à-plusieurs : permet la mise à jour automatique de plusieurs périphériques iDRAC6, sans intervention manuelle
- 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 iDRAC6

iDRAC6 intègre les fonctionnalités de sécurité suivantes :

- Authentification des utilisateurs via Microsoft Active Directory (en option) ou via les ID d'utilisateur et les mots de passe stockés sur le matériel
- Autorité basée sur le rôle, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- Configuration d'un ID d'utilisateur et d'un mot de passe via l'interface Web, SM-CLP ou l'interface RACADM locale
- SM-CLP et interfaces Web prenant en charge le cryptage 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté) à l'aide de la norme SSL 3.0
- Configuration du délai d'expiration de la session (en secondes) via l'interface Web ou SM-CLP
- Ports IP configurables (si applicable)

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

- Secure Shell (SSH) qui utilise une couche de transport cryptée pour une sécurité plus élevée
- Nombre maximal d'échecs d'ouverture de session par adresse IP, avec blocage de l'ouverture de session à partir de l'adresse IP lorsque la limite est dépassée
- Plage d'adresses IP limitée pour les clients se connectant à iDRAC6

Améliorations du micrologiciel iDRAC6

En outre, d'importantes améliorations ont été apportées au code :

- Améliorations majeures de la performance de recherche d'Active Directory
- Amélioration de la réactivité de la pile de mise en réseau TCP-IP
- Amélioration de l'interface de condition d'intégrité entre iDRAC6 et CMC
- Améliorations de la sécurité à l'aide de multiples outils d'analyse tiers

---

Plateformes prises en charge

iDRAC6 prend en charge les systèmes PowerEdge suivants dans l'enceinte du système Dell PowerEdge M1000e :

- PowerEdge M610
- PowerEdge M710

Concernant les dernières plateformes prises en charge, voir le fichier « Lisez-moi » iDRAC6 disponible sur le site Web de support Dell à l'adresse suivante : **support.dell.com/manuals**.

Systèmes d'exploitation pris en charge

Tableau 1-1 répertorie les systèmes d'exploitation prenant en charge iDRAC6.

Consultez la *Matrice de prise en charge des logiciels des systèmes Dell* disponible sur le site Web de support Dell à l'adresse **support.dell.com/manuals** pour connaître les dernières informations.

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

Gamme de systèmes d'exploitation	Système d'exploitation
Sous 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 (64 bits) avec SP2 Microsoft Windows Storage Server 2003 R2, éditions x64 Express, Workgroup, Standard 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) MS HyperV 2008 **REMARQUE :** Lorsque vous installez Windows Server 2003 avec Service Pack 1, gardez à l'esprit que des modifications ont été apportées aux paramètres de sécurité DCOM. Pour plus d'informations, consultez l'article 903220 sur le site Web de support de Microsoft à l'adresse **support.microsoft.com/kb/903220**.

Red Hat® Enterprise Linux®	Enterprise Linux WS, ES et AS (version 4) (x86 et x86_64) Enterprise Linux 5 (x86 et x86_64)
SUSE® Linux	Enterprise Server 10 (Gold) (x86_64)
VMware	ESX 3.5 U4

Navigateurs Web pris en charge

Tableau 1-2 répertorie les navigateurs Web pris en charge en tant que clients iDRAC6.

Consultez le fichier « Lisez-moi » iDRAC6 et la *Matrice de prise en charge des logiciels des systèmes Dell* disponibles sur le site Web de support Dell à l'adresse **support.dell.com/manuals** pour connaître les dernières informations.

REMARQUE : En raison de graves défauts de sécurité, la prise en charge de SSL 2.0 a été abandonnée. Pour que votre navigateur fonctionne correctement, vous devez activer SSL 3.0.

Tableau 1-2. Navigateurs Web pris en charge

Système d'exploitation	Navigateur Web pris en charge
Windows	Internet Explorer® 6.0 avec Service Pack 2 (SP2) uniquement pour Windows XP et Windows 2003 R2 SP2 Internet Explorer 7.0 pour Windows Vista®, Windows XP, Windows 2003 R2 SP2 et Windows Server 2008 uniquement Mozilla Firefox 2.0/3.0 pour Windows (console Java vKVM/vMedia uniquement)
Linux	Mozilla Firefox 2.0/3.0 sur Red Hat Enterprise Linux 4 et 5 (32 bits ou 64 bits) et SUSE Linux Enterprise Server 10 (32 bits ou 64 bits)

Connexions d'accès à distance prises en charge

Tableau 1-3 répertorie les fonctionnalités de connexion.

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

Connexion	Fonctionnalités
NIC iDRAC6	• Ethernet 10 Mb/s, 100 Mb/s ou 1 Gb/s via le port Ethernet Gb 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 d'iDRAC6, le démarrage système, la réinitialisation, la mise sous tension et les commandes d'arrêt • Prise en charge des utilitaires IPMI, tels que IPMItool et ipmish

Ports iDRAC6

Tableau 1-4 répertorie les ports sur lesquels iDRAC6 écoute les connexions. Tableau 1-5 identifie les ports qu'iDRAC6 utilise comme client. Ces informations sont requises pour ouvrir des pare-feux afin de pouvoir accéder à distance à iDRAC6.

Tableau 1-4. Ports d'écoute de serveur iDRAC6

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

Tableau 1-5. Ports clients iDRAC6

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

Autres documents utiles

En plus de ce *Guide d'utilisation*, les documents suivants fournissent des informations supplémentaires sur la configuration et l'utilisation d'iDRAC6 dans votre système :

- L'aide en ligne d'iDRAC6 fournit des informations sur l'utilisation de l'interface Web.
- Le *Guide d'utilisation de la version 2.0 du micrologiciel Dell Chassis Management Controller* et le *Guide de référence Administrateur du micrologiciel Dell Chassis Management Controller, version 2.0* fournissent des informations sur l'utilisation du contrôleur qui gère tous les modules du châssis contenant votre serveur PowerEdge.
- Le *Guide d'utilisation de Dell OpenManage IT Assistant* fournit des informations relatives à l'utilisation d'IT Assistant.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator* donne des informations sur l'installation et l'utilisation de Server Administrator.
- Le *Guide d'utilisation des progiciels Dell Update Package* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Package dans le contexte de la stratégie de mise à jour de votre système.
- Le *Guide d'utilisation de Dell Unified Server Configurator* fournit des informations sur l'installation et l'exploitation d'Unified Server Configurator.

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

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

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

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

Retour à la page du sommaire

Retour à la page du sommaire

Configuration d'iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Cette section contient des informations sur la façon d'accéder à iDRAC6 et de configurer votre environnement de gestion pour utiliser iDRAC6.

Avant de commencer

Réunissez les éléments suivants avant de configurer iDRAC6 :

- *Guide d'utilisation du micrologiciel Dell Chassis Management Controller*
- DVD Dell Systems Management Tools and Documentation

Le DVD *Dell Systems Management Tools and Documentation* inclut les composants suivants :

- Racine du DVD : contient Dell Systems Build and Update Utility, qui fournit des informations de configuration du serveur et d'installation du système
- SYSMGMT : contient les produits Systems Management Software, dont Dell OpenManage Server Administrator
- DOCS : contient la documentation des produits Systems Management Software, des périphériques et des contrôleurs RAID
- SERVICE : contient les outils dont vous avez besoin pour configurer votre système ainsi que les derniers diagnostics et pilotes optimisés par Dell pour votre système

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

Interfaces de configuration d'iDRAC6

Vous pouvez configurer iDRAC6 à l'aide de l'utilitaire de configuration iDRAC6, de l'interface Web iDRAC6, de la CLI RACADM locale ou de la CLI SM-CLP. La CLI RACADM locale est disponible une fois que vous avez installé le système d'exploitation et le logiciel Dell OpenManage sur le serveur géré. Tableau 2-1 décrit ces interfaces.

Pour une sécurité accrue, l'accès à la configuration iDRAC6 via l'utilitaire de configuration iDRAC6 ou la CLI RACADM locale peut être désactivé à l'aide d'une commande RACADM (consultez la section « Présentation de la sous-commande RACADM ») ou depuis l'interface utilisateur (consultez la section « Activation ou désactivation de l'accès à la configuration locale »).

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

Tableau 2-1. Interfaces de configuration

Interface	Description
Configuration d'iDRAC6 configuration iDRAC	L'utilitaire de configuration iDRAC6, 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 iDRAC6	L'interface Web iDRAC6 est une application de gestion basée sur un navigateur que vous pouvez utiliser pour gérer iDRAC6 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 locaux iDRAC6 et le lancement de l'interface Web du CMC et des sessions de redirection de console.
Interface Web CMC	Outre la surveillance et la gestion du châssis, l'interface Web du CMC peut être utilisée pour afficher la condition d'un serveur géré, configurer les paramètres réseau iDRAC6 et pour démarrer, arrêter ou réinitialiser le serveur géré.
Écran LCD du châssis	L'écran LCD du châssis contenant iDRAC6 peut être utilisé pour afficher la condition de niveau élevé des serveurs dans le châssis. Lors de la configuration initiale du CMC, l'Assistant Configuration vous permet d'activer la configuration DHCP de la mise en réseau iDRAC6.
RACADM locale	L'interface de ligne de commande RACADM locale s'exécute sur le serveur géré. Elle est accessible depuis l'iKVM ou une session de redirection de console initiée à partir de l'interface Web iDRAC6. 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 iDRAC6. Vous pouvez inspecter les données du capteur, les enregistrements du journal des événements système et les valeurs de condition et de configuration actuelles conservées dans iDRAC6. Vous pouvez modifier les valeurs de configuration iDRAC6, gérer les utilisateurs locaux, activer et désactiver les fonctionnalités et exécuter des fonctions d'alimentation, comme l'arrêt ou le redémarrage du serveur géré.
CLI de l'iVM	L'interface de ligne de commande du média virtuel iDRAC6 (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 la mise en oeuvre du protocole de ligne de commande Server Management (SM-CLP) du groupe de travail de gestion de serveur incorporé dans iDRAC6. La ligne de commande SM-CLP est accessible en ouvrant une session sur iDRAC6 à l'aide de Telnet ou de

	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. Consultez la section « Équivalences RACADM et SM-CLP » pour obtenir un comparatif des commandes RACADM et SM-CLP.
IPMI	IPMI définit une méthode standard permettant aux sous-systèmes de gestion intégrés, comme iDRAC6, de communiquer avec d'autres systèmes intégrés et d'autres applications de gestion. Vous pouvez utiliser l'interface Web iDRAC6, SM-CLP ou les commandes RACADM pour configurer les filtres d'événements sur plateforme (PEF) et les interruptions d'événements sur plateforme (PET) IPMI. Le PEF oblige iDRAC6 à effectuer des actions spécifiques (par exemple, le redémarrage du serveur géré) lorsqu'il détecte une condition. Le PET ordonne à iDRAC6 d'envoyer des alertes IPMI ou par e-mail lorsqu'il détecte des événements ou des conditions spécifiés. Vous pouvez également utiliser des outils IPMI standard tels que **IPMItool** et **ipmish** avec iDRAC6 lorsque vous activez IPMI sur le LAN.

Tâches de configuration

Cette section est une présentation des tâches de configuration pour la station de gestion, iDRAC6 et le serveur géré. Les tâches à effectuer incluent la configuration d'iDRAC6 afin de pouvoir l'utiliser à distance, la configuration des fonctionnalités d'iDRAC6 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 logiciels. Voir « Configuration de la station de gestion ».

Configurer la mise en réseau iDRAC6

Activez le réseau iDRAC6 et configurez les adresses IP, de masque réseau, de passerelle et DNS.

REMARQUE : L'accès à la configuration iDRAC6 via l'utilitaire de configuration iDRAC6 ou la CLI RACADM locale peut être désactivé au moyen d'une commande RACADM (consultez la section « Présentation de la sous-commande RACADM ») ou depuis l'interface utilisateur (consultez la section « Activation ou désactivation de l'accès à la configuration locale »).

REMARQUE : La modification des paramètres réseau iDRAC6 met fin à toutes les connexions réseau actuelles sur iDRAC6.

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 iDRAC6.

REMARQUE : L'écran LCD peut être utilisé pour activer DHCP pour configurer le réseau iDRAC6. Si vous souhaitez attribuer des adresses statiques, vous devez utiliser l'utilitaire de configuration iDRAC6 ou l'interface Web du CMC.

- Écran LCD du châssis : consultez le *Guide d'utilisation du micrologiciel Dell Chassis Management Controller*.
- Utilitaire de configuration iDRAC6 : consultez la section « Utilisation de l'utilitaire de configuration iDRAC6 »
- Interface Web du CMC : consultez la section « Configuration de la mise en réseau via l'interface Web CMC »
- RACADM : consultez la section « cfgLanNetworking »

Configurer les utilisateurs iDRAC6

Configurez les utilisateurs locaux iDRAC6 ainsi que les droits. iDRAC6 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 iDRAC6 (configure l'utilisateur d'administration uniquement) : consultez la section «Utilisation de l'utilitaire de configuration iDRAC6 »
- Interface Web iDRAC6 : consultez la section « Ajout et configuration des utilisateurs iDRAC6 »
- RACADM : consultez la section « Ajout d'un utilisateur iDRAC6 »

REMARQUE : Lorsque vous utilisez iDRAC6 dans un environnement Active Directory, les noms d'utilisateur que vous créez doivent respecter la convention d'attribution de noms Active Directory en vigueur.

Configurer Active Directory

Outre les utilisateurs locaux iDRAC6, vous pouvez utiliser Microsoft® Active Directory® pour authentifier les ouvertures de session utilisateur iDRAC6.

Pour plus d'informations, voir « Utilisation d'iDRAC6 avec Microsoft Active Directory ».

REMARQUE : Lorsque vous utilisez iDRAC6 dans un environnement Active Directory, assurez-vous que vos noms d'utilisateur respectent la convention d'attribution de noms Active Directory en vigueur.

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 iDRAC6 : consultez la section « Configuration du filtrage IP et du blocage IP »
- RACADM : consultez les sections « Configuration du filtrage IP (plage IP) » et « Configuration du blocage IP »

Configurer les événements sur plateforme

Les événements sur plateforme se produisent lorsque iDRAC6 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 le redémarrage du serveur géré, lorsqu'un événement est détecté.

- Interface Web iDRAC6 : consultez la section « Configuration des filtres d'événements sur plateforme (PEF) »
- RACADM : consultez la section « 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 iDRAC6 : consultez la section « Configuration des filtres d'événements sur plateforme (PEF) »
- RACADM : consultez la section « Configuration du PET »

Activation ou désactivation de l'accès à la configuration locale

L'accès aux paramètres de configuration critiques, comme la configuration réseau et les privilèges utilisateur, peut être désactivé. Une fois l'accès désactivé, le paramètre persiste d'un réamorçage à l'autre. L'accès en écriture à la configuration est bloqué pour le programme de la RACADM locale et l'utilitaire de configuration iDRAC6 (au démarrage). L'accès Web aux paramètres de configuration est libre et les données de configuration peuvent toujours être visualisées. Pour des informations sur l'interface Web iDRAC6, consultez la section « Activation ou désactivation de l'accès à la configuration locale ». Pour les commandes cfgRacTuning, consultez la section « cfgRacTuning ».

Configurer les services iDRAC6

Activez ou désactivez les services réseau iDRAC6, comme Telnet, SSH et l'interface Web Server, et reconfigurez les ports et les autres paramètres de services.

- Interface Web iDRAC6 : consultez la section « Configuration des services iDRAC6 »
- RACADM : consultez la section « Configuration de services Telnet et SSH iDRAC6 via RACADM local »

Configurer le protocole Secure Sockets Layer (SSL)

Configurez SSL pour Web Server iDRAC6.

- Interface Web iDRAC6 : consultez la section « Secure Sockets Layer (SSL) »
- RACADM : consultez les sections « cfgRacSecurity », « sslcsrgen », « sslcertupload », « sslcertdownload » et « 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 iDRAC6 : consultez la section « Configuration et utilisation du média virtuel »
- Utilitaire de configuration iDRAC6 : consultez la section « Configuration du média virtuel »

Configurer une carte de média VFlash

Installez et configurez une carte de média VFlash à utiliser avec iDRAC6.

- Interface Web iDRAC6 : consultez la section « Configuration d'une carte de support VFlash pour utilisation avec iDRAC6 »

Installer le logiciel Managed Server

Installez le système d'exploitation 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 : consultez la section « Installation du logiciel sur le serveur géré »
- iVMCLI : consultez la section « Utilisation de l'utilitaire d'interface de ligne de commande du média virtuel »

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

Configurez le serveur géré de manière à ce qu'iDRAC6 puisse capturer l'image de l'écran après un plantage ou un blocage du système d'exploitation.

- Serveur géré : consultez les sections « Configuration du serveur géré pour la saisie de l'écran du dernier plantage » et « Désactivation de l'option Redémarrage automatique de Windows »

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

REMARQUE : Vous devez disposer de droits d'administrateur de configuration du châssis pour pouvoir configurer les paramètres réseau iDRAC6 depuis le CMC.

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

REMARQUE : Vous pouvez trouver l'adresse IP du CMC dans l'interface Web iDRAC6 en cliquant sur **Système→ Accès à distance→ CMC**. Vous pouvez également lancer l'interface Web du CMC à partir de cet écran.

Lancement de l'interface Web iDRAC6 depuis le CMC

CMC fournit une gestion limitée des composants individuels de châssis tels que les serveurs. Pour une gestion complète de ces composants individuels, le CMC fournit un point de lancement pour l'interface Web iDRAC6 du serveur.

Pour lancer iDRAC6 depuis l'écran **Serveurs** :

1. Connectez-vous à l'interface Web CMC.
2. Dans l'arborescence du système, sélectionnez **Serveurs**.

   L'écran **Condition des serveurs** apparaît.
3. Cliquez sur l'icône **Lancer l'interface utilisateur iDRAC** pour le serveur que vous voulez gérer.

Vous pouvez également lancer l'interface Web iDRAC6 pour un serveur unique à l'aide de la liste **Serveurs** dans l'arborescence du système :

1. Connectez-vous à l'interface Web CMC.
2. Développez **Serveurs** dans l'arborescence du système.

   Tous les serveurs (1 à 16) s'affichent dans la liste développée **Serveurs**.
3. Cliquez sur le serveur dont vous souhaitez afficher les informations.

   L'écran **Condition des serveurs** pour le serveur que vous avez sélectionné s'affiche.
4. Cliquez sur l'icône **Lancer l'interface utilisateur iDRAC**.

Connexion directe

Utilisez la fonctionnalité d'authentification unique pour lancer l'interface Web iDRAC6 depuis le CMC sans avoir à ouvrir une session une deuxième fois. Les stratégies d'authentification unique sont décrites ci-dessous.

- Un utilisateur du CMC pour lequel **Server Administrator** est défini sous **Droits d'utilisateur** ouvrira automatiquement une session sur l'interface Web iDRAC6 à l'aide de l'authentification unique. Une fois la session ouverte, l'utilisateur reçoit automatiquement des droits d'administrateur iDRAC6. Cela est vrai même si le même utilisateur n'a pas de compte sur iDRAC6 ou si le compte n'a pas de droits d'administrateur.
- Un utilisateur CMC pour lequel Server Administrator n'est pas défini sous Droits d'utilisateur, mais qui a le même compte sur iDRAC6, ouvrira

automatiquement une session sur iDRAC6 à l'aide de l'authentification unique. Une fois qu'il a ouvert une session sur l'interface Web iDRAC6, cet utilisateur reçoit les droits qui ont été créés pour le compte iDRAC6.

REMARQUE : Dans ce contexte, « le même compte » signifie que l'utilisateur possède le même nom d'ouverture de session et le même mot de passe pour le CMC que pour iDRAC6. Un utilisateur ayant le même nom d'ouverture de session, mais un mot de passe différent, ne sera pas reconnu comme utilisateur valide.

- Un utilisateur CMC pour lequel Server Administrator n'est pas défini sous Droits d'utilisateur et qui n'a pas le même compte sur iDRAC6, n'ouvrira *pas* automatiquement une session sur iDRAC6 à l'aide de l'authentification unique. Cet utilisateur est dirigé vers l'écran d'ouverture de session de iDRAC6 après avoir cliqué sur **Lancer l'interface utilisateur iDRAC**.

  REMARQUE : Dans ce cas, les utilisateurs peuvent être invités à ouvrir une session sur iDRAC6.

REMARQUE : Si le LAN réseau iDRAC6 est désactivé (LAN activé = non), l'authentification unique n'est pas disponible.

REMARQUE : Si le serveur est retiré du châssis, que l'adresse IP iDRAC est modifiée ou qu'un problème de connexion réseau iDRAC6 se produit, un écran d'erreur peut s'afficher lorsque l'utilisateur clique sur l'icône **Lancer l'interface utilisateur iDRAC**.

Configuration de la mise en réseau pour iDRAC6

1. Cliquez sur **Système** → **Accès à distance** → **IDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**.

   Pour activer ou désactiver Communications série sur le LAN :

   a. Cliquez sur **Connexion série sur le réseau local**.

      L'écran **Communications série sur le LAN** apparaît.

   b. Cochez la case **Activer les communications série sur le LAN**. Vous pouvez également modifier les paramètres **Débit en bauds** et **Limite du niveau de droit du canal**.

   c. Cliquez sur **Appliquer**.

   Pour activer ou désactiver IPMI sur le LAN :

   a. Cliquez sur **Réseau**.

      L'écran **Configuration réseau** apparaît.

   b. Cliquez sur **Paramètres LAN IPMI**.

   c. Cochez la case **Activer IPMI sur le LAN.** Vous pouvez également modifier les paramètres **Limite du niveau de droit du canal** et **Clé de cryptage**.

   d. Cliquez sur **Appliquer**.

   Pour activer ou désactiver DHCP :

   a. Cliquez sur **Réseau**.

      L'écran **Configuration réseau** apparaît.

   b. Cliquez sur **Paramètres réseau**.

      - Pour utiliser DHCP pour l'adresse IP du NIC, cochez la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
      - Pour utiliser DHCP pour obtenir les adresses de serveur DNS, cochez la case **Utiliser DHCP pour obtenir des adresses de serveur DNS**.

   c. Cliquez sur **Appliquer**.

REMARQUE : Si vous choisissez de ne pas activer DHCP, vous devez saisir l'adresse IP statique, le masque de réseau et la passerelle par défaut pour le serveur.

Visualisation des connexions Fabric des cartes mezzanines FlexAddress

Le M1000e inclut FlexAddress, un système de mise en réseau multistandard et multiniveaux avancé. FlexAddress permet d'utiliser des noms mondiaux et des adresses MAC (WWN/MAC) persistants assignés au châssis pour chaque connexion de port de serveur géré.

REMARQUE : Afin d'éviter des erreurs pouvant empêcher la mise sous tension du serveur géré, vous *devez* avoir installé le type correct de carte mezzanine pour chaque port et chaque connexion Fabric.

La fonctionnalité FlexAddress est configurée à l'aide de l'interface Web du CMC. Pour plus d'informations sur la fonctionnalité FlexAddress et sa configuration, consultez votre *Guide d'utilisation de la version 2.0 du micrologiciel Dell Chassis Management Controller*.

Lorsque la fonctionnalité FlexAddress a été activée et configurée pour le châssis, cliquez sur **Système**→ **Propriétés**→ **WWN/MAC** pour afficher une liste des cartes mezzanines installées, les Fabric et les ports auxquels elles sont connectées, l'emplacement des ports Fabric, le type de Fabric ainsi que les adresses MAC configurées pour les serveurs ou attribuées au châssis pour chaque port Ethernet intégré installé et pour chaque port de carte mezzanine facultatif.

Pour visualiser une liste des cartes mezzanines installées, le type de carte mezzanine installée et si FlexAddress est configuré, cliquez sur **Système**→ **Propriétés**→ **Résumé**.

Mise à jour du micrologiciel iDRAC6

La mise à jour du micrologiciel iDRAC6 installe une nouvelle image de micrologiciel dans la mémoire Flash. Vous pouvez mettre à jour le micrologiciel à l'aide de l'une des méthodes suivantes :

- Commande **load** SM-CLP
- Interface Web iDRAC6
- Progiciel de mise à jour Dell (pour Linux ou Microsoft Windows)
- Utilitaire de mise à jour du micrologiciel iDRAC6 DOS
- Interface Web du CMC

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 prendre en charge les diverses méthodes de mise à jour disponibles.

Pour mettre à jour le micrologiciel iDRAC6 à l'aide de l'interface Web iDRAC6 ou SM-CLP, ou pour récupérer iDRAC6 à l'aide de l'interface Web du CMC, téléchargez l'image binaire qui se présente sous la forme d'une archive à extraction automatique.

Pour mettre à jour le micrologiciel iDRAC6 à partir du serveur géré, téléchargez le progiciel Dell Update Package (DUP) spécifique au système d'exploitation qui s'exécute sur le serveur dont vous mettez à jour iDRAC6.

Pour mettre à jour le micrologiciel iDRAC6 à l'aide de l'utilitaire de mise à jour du micrologiciel iDRAC6 DOS, téléchargez l'utilitaire de mise à jour et l'image binaire, qui se présentent sous la forme d'archives à extraction automatique.

Exécution de la mise à jour du micrologiciel

REMARQUE : Lorsque la mise à jour du micrologiciel iDRAC6 commence, toutes les sessions iDRAC6 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 du micrologiciel iDRAC6. 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 iDRAC6. Voir « Mise à jour du micrologiciel iDRAC6 via SM-CLP ».

Lorsque vous utilisez l'interface Web iDRAC6 ou l'interface Web du 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 iDRAC6 ».

REMARQUE : L'interface Web iDRAC6 vous permet également de rétablir les paramètres d'usine de la configuration iDRAC6.

Vous pouvez utiliser l'interface Web du CMC ou la RACADM du CMC pour mettre à jour le micrologiciel iDRAC6. Cette fonctionnalité est disponible lorsque le micrologiciel iDRAC6 est en mode Normal ainsi que lorsqu'il est corrompu. Voir « Mise à jour du micrologiciel iDRAC6 à l'aide de CMC ».

REMARQUE : Lorsque le CMC a mis à jour le micrologiciel iDRAC6, iDRAC6 génère de nouvelles clés SHA1 et MD5 pour le certificat SSL. Étant donné que les clés diffèrent de celles du navigateur Web ouvert, toutes les fenêtres du navigateur qui sont connectées à iDRAC6 doivent être fermées une fois la mise à jour du micrologiciel terminée. Si les fenêtres du navigateur ne sont pas fermées, un message d'erreur **Certificat invalide** s'affiche.

REMARQUE : Si vous antidatez le micrologiciel iDRAC6 à une version antérieure, vous devez supprimer le plug-in ActiveX® du navigateur Internet Explorer existant sur n'importe quelle station de gestion Windows afin que le micrologiciel puisse installer une version compatible du plug-in ActiveX. Pour plus d'informations, voir « Suppression du plug-in ActiveX ».

Suppression du plug-in ActiveX

Vous devez supprimer le plug-in ActiveX du navigateur Internet Explorer existant sur n'importe quelle station de gestion Windows afin que le micrologiciel puisse installer une version compatible du plug-in ActiveX.

Pour supprimer le plug-in ActiveX dans Internet Explorer 6 :

1. Accédez à **C:\WINDOWS\Downloaded Program Files**.
2. Supprimez le fichier **DELL IDRAC 11G AVCView**.

Pour supprimer le plug-in ActiveX dans Internet Explorer 7 :

1. Ouvrez Internet Explorer 7.

2. Appuyez sur la touche <Alt> pour afficher la barre de menus, si besoin est.
3. Cliquez sur **Outils**→ **Gérer les extensions**→ **Activer ou désactiver les extensions**.
4. Dans la fenêtre **Gérer les extensions**, sélectionnez **Contrôles ActiveX téléchargés (32 bits)** dans le menu déroulant **Afficher**.
5. Dans la liste **Activé**, cliquez sur **DELL IDRAC 11G AVCView**, puis sur le bouton **Supprimer** dans la section **Supprimer ActiveX**.
6. Cliquez sur **OK**.

Utilisation de l'interface Web iDRAC6

PRÉCAUTION : Si le micrologiciel iDRAC6 devient corrompu, ce qui peut être le cas si la progression de la mise à jour du micrologiciel iDRAC6 est interrompue avant qu'elle ne soit terminée, vous pouvez récupérer iDRAC6 à l'aide de l'interface Web iDRAC6.

REMARQUE : Par défaut, la mise à jour du micrologiciel conserve les paramètres actuels iDRAC6. Lors du processus de mise à jour, vous avez la possibilité de rétablir les paramètres d'usine de la configuration iDRAC6. 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 iDRAC6.

1. Démarrez l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ **iDRAC**.
3. Cliquez sur l'onglet **Mettre à jour**.

   L'écran **Mise à jour du micrologiciel** apparaît.

   REMARQUE : Pour mettre à jour le micrologiciel, iDRAC6 doit mis en mode de mise à jour. Lorsqu'il se trouve sur ce mode, iDRAC6 se réinitialise automatiquement, même si vous annulez le processus de mise à jour.

4. Dans la section **Télécharger (étape 1 de 4)**, cliquez sur **Parcourir pour localiser** l'image de micrologiciel que vous avez téléchargée. Vous pouvez également saisir le chemin dans le champ textuel. Par exemple :

   `C:\Updates\V2.0\<nom_de_l'image>`.

   Par défaut, le nom de l'image du micrologiciel est **firmimg.imc**.

5. Cliquez sur **Télécharger**.

   Le fichier se télécharge sur iDRAC6. This may take several minutes to complete.

   REMARQUE : Lors du processus de téléchargement, vous pouvez abandonner le processus de mise à niveau du micrologiciel en cliquant sur **Annuler**. Le fait de cliquer sur **Annuler** rétablit le mode de fonctionnement normal d'iDRAC6.

   Lorsque le téléchargement est terminé, l'écran **Mise à jour du micrologiciel - Validation (page 2 de 4)** s'affiche.

   - Si le fichier image s'est téléchargé et a réussi toutes les vérifications, un message apparaît indiquant que l'image du micrologiciel a été vérifiée.
   - Si l'image ne s'est pas téléchargée correctement ou si elle n'a pas réussi les vérifications, la mise à jour du micrologiciel retourne à l'écran **Mise à jour du micrologiciel**. Vous pouvez essayer de mettre à nouveau iDRAC6 à niveau ou cliquer sur **Annuler** pour rétablir le mode de fonctionnement normal d'iDRAC6.

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

6. Par défaut, l'option **Préserver la configuration** est activée (cochée) pour préserver les paramètres actuels sur iDRAC6 après une mise à niveau. Si vous ne voulez pas que les paramètres soient préservés, décochez la case **Préserver la configuration**.
7. Cliquez sur **Démarrer la mise à jour** pour démarrer le processus de mise à niveau. N'interrompez pas le processus de mise à niveau.
8. Dans la fenêtre **Mise à jour du micrologiciel - Mise à jour (page 3 de 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**.
9. Une fois la mise à jour du micrologiciel terminée, la fenêtre **Mise à jour du micrologiciel - Résultats de la mise à jour (page 4 de 4)** apparaît et iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre actuelle du navigateur et vous reconnecter à iDRAC6 avec une nouvelle fenêtre du navigateur.

Utilisation de l'utilitaire de mise à jour DOS

Pour mettre à jour le micrologiciel iDRAC6 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 iDRAC6 à l'aide du fichier image du 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 le nom de fichier de l'image du 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.

REMARQUE : Si vous saisissez des arguments incorrects pour la commande **idrac16d** ou indiquez l'option `-h`, il est possible que vous remarquiez une option supplémentaire, `-nopresconfig`, 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 à moins qu'un représentant du support de Dell ne vous y invite explicitement, car elle *supprime* toutes vos informations existantes de la configuration iDRAC6, comme les adresses IP, les utilisateurs et les mots de passe.

Vérification de la signature numérique

Une signature numérique est utilisée pour authentifier l'identité du signataire d'un fichier et 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 de confiance gpg en exécutant la commande suivante :

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

   REMARQUE : Vous devez avoir 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. Entrez 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)(Groupe de produit) <linux-security@dell.com>
      Primary Key fingerprint(Empreinte de clé primaire) : 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.)(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 = I don't know or won't say (Je ne sais pas ou ne souhaite pas me prononcer)
        2 = I do NOT trust (Je NE fais PAS confiance)
        3 = I trust marginally (Je fais un peu confiance)
        4 = I trust fully (Je fais entièrement confiance)
        5 = I trust ultimately (Je fais définitivement confiance)
        m = back to the main menu (retour au menu principal)

      Your decision? (Votre décision ?)
      ```

   d. Tapez `5`, puis appuyez sur <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] ([O/N]))
      ```

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

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

   Vous ne devez importer et valider la clé publique qu'une seule fois.

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**. Par exemple, l'image du micrologiciel iDRAC6 est associée à un fichier **.sign** (**IDRAC_FRMW_LX_2.0.BIN.sign**), qui est inclus dans l'archive à extraction automatique avec l'image du micrologiciel (**IDRAC_FRMW_LX_2.0.BIN**). 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 la signature du progiciel DUP Linux> <Nom de fichier du progiciel DUP Linux>`

L'exemple suivant illustre les étapes à suivre pour vérifier un progiciel de mise à jour du Dell PowerEdge™ M610 iDRAC :

1. Téléchargez les deux fichiers suivants à partir de **support.dell.com** :
   - IDRAC_FRMW_LX_2.0.BIN.sign
   - IDRAC_FRMW_LX_2.0.BIN

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

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

   Le message suivant apparaît :

   ```
   gpg : Key (clé) 23B66A9D : « Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com> » not changed (inchangé)
   gpg : Total number processed (nombre total traité) : 1
   gpg : unchanged (inchangé) : 1
   ```

3. Définissez le niveau de confiance GPG pour la clé publique Dell, si vous ne l'avez pas déjà fait.
   a. Entrez la commande suivante :

      `gpg --edit-key 23B66A9D`

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

      ```
      fpr
      trust
      ```

   c. Tapez 5, puis appuyez sur <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 PowerEdge M610 iDRAC en exécutant la commande suivante :

   ```
   gpg --verify IDRAC_FRMW_LX_2.0.BIN.sign IDRAC_FRMW_LX_2.0.BIN
   ```

   Le message suivant apparaît :

   ```
   gpg : Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D gpg: Good signature from "Dell, Inc. (Product Group)
   (Signature le ven 11 juil 15:03:47 2008 CDT à l'aide de l'ID de clé DSA 23B66A9D
   gpg : Signature correcte de « Dell, Inc. (Groupe de produits)) <linux-security@dell.com> »
   ```

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

   ```
   gpg : 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 (AVERTISSEMENT : Cette clé n'est pas certifiée avec une
   signature de confiance !
   gpg : Il n'y a aucune indication que la signature appartienne au propriétaire.
   Empreinte de clé primaire : 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D)
   ```

Effacer la mémoire cache de votre navigateur

Pour pouvoir utiliser les fonctionnalités du dernier iDRAC6, vous devez effacer la mémoire cache du navigateur pour effacer/supprimer les *anciennes* pages Web susceptibles d'être stockées sur le système.

Internet Explorer 6

1. Démarrez Internet Explorer.

2. Cliquez sur **Outils**, puis sur **Options Internet**.

La fenêtre **Options Internet** s'affiche.

3. Cliquez sur l'onglet **Général**.
4. Sous **Fichiers Internet temporaires**, cliquez sur **Supprimer les fichiers**.

   La fenêtre **Supprimer les fichiers** apparaît.

5. Cliquez pour cocher **Supprimer tout le contenu hors connexion**, puis cliquez sur **OK**.
6. Cliquez sur **OK** pour fermer la fenêtre **Options Internet**.

Internet Explorer 7

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils**, puis sur **Options Internet**...

   La fenêtre **Options Internet** s'affiche.

3. Cliquez sur l'onglet **Général**.
4. Sous **Navigation dans l'historique**, cliquez sur **Supprimer...**

   La fenêtre **Supprimer les fichiers** apparaît.

5. Cliquez sur **Supprimer des fichiers** en regard de **Fichiers Internet temporaires**.
6. Cliquez sur **Fermer**, puis sur **OK** pour quitter la fenêtre **Options Internet**.

Firefox.

1. Démarrez Firefox.
2. Cliquez sur **Modifier→ Préférences**.
3. Cliquez sur l'onglet **Confidentialité**.
4. Cliquez sur **Effacer la mémoire cache maintenant**.
5. Cliquez sur **Close** (Fermer).

Mise à jour du progiciel de réparation de l'USC

Consultez le *Guide d'utilisation de Dell Unified Server Configurator* pour des informations sur la mise à jour du progiciel de réparation de l'USC depuis l'interface Web iDRAC6.

Configuration d'iDRAC6 pour l'utiliser avec IT Assistant

Dell OpenManage IT Assistant peut découvrir des périphériques gérés qui sont conformes au protocole SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]) v1 et v2c et à Intelligent Platform Management Interface (IPMI) v2.0.

iDRAC6 est conforme à IPMI v2.0. Cette section décrit les étapes de configuration d'iDRAC6 pour la découverte et la surveillance par IT Assistant. La configuration peut se faire de deux manières : via l'utilitaire de configuration iDRAC6 et via l'interface Web graphique iDRAC6.

Utilisation de l'utilitaire de configuration iDRAC6 pour activer la découverte et la surveillance

Pour configurer iDRAC6 pour la découverte et l'envoi d'une interruption d'alerte IPMI au niveau de l'utilitaire de configuration iDRAC6, redémarrez votre serveur géré (lame) et observez sa mise sous tension à l'aide de l'iKVM et d'un moniteur et d'un clavier de console distants ou d'une connexion série sur le LAN (SOL). Lorsque Press (Appuyez sur) <Ctrl-E> for Remote Access Setup (pour configurer l'accès à distance) <Ctrl-E> apparaît, appuyez sur <Ctrl><E>.

Lorsque l'écran **Utilitaire de configuration de l'iDRAC** apparaît, utilisez les touches fléchées pour défiler vers le bas.

1. Activez **IPMI sur le LAN**.
2. Saisissez **la clé de cryptage RMCP+** de votre site, si elle est utilisée.

REMARQUE : Consultez votre administrateur réseau ou votre responsable des technologies de l'information principal pour discuter de la mise en uvre de cette option car elle ajoute une protection de sécurité précieuse et elle doit être mise en uvre au niveau du site pour fonctionner correctement.

3. Dans **Paramètres du LAN**, appuyez sur <Entrée> pour accéder au sous- écran. Utilisez les touches vers le haut et vers le bas pour naviguer.
4. Basculez **Alerte LAN activée** sur **Marche** à l'aide de la barre espace.
5. Saisissez l'adresse IP de votre Management Station dans **Destination de l'alerte 1**.
6. Saisissez une chaîne de nom dans **Nom d'iDRAC6** en respectant une convention d'attribution de nom cohérente sur l'ensemble de votre centre de données. La chaîne par défaut est `iDRAC6-{`*`numéro de service`*`}`.

Quittez l'utilitaire de configuration iDRAC6 en appuyant sur <Échap>, <Échap>, puis sur <Entrée> pour sauvegarder vos modifications. Votre serveur va maintenant démarrer en mode de fonctionnement normal et IT Assistant va le découvrir pendant l'exécution de la découverte programmée suivante.

Utilisation de l'interface Web iDRAC6 pour activer la découverte et la surveillance

La découverte IPMI peut également être activée via l'interface Web distante :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6 en utilisant un nom d'ouverture de session et un mot de passe possédant des droits d'administrateur.
3. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ **iDRAC**.
4. Cliquez sur l'onglet **Réseau/Sécurité**.

   L'écran **Configuration réseau** apparaît.
5. Cliquez sur **Paramètres LAN IPMI**.
6. Vérifiez que la case **Activer IPMI sur le LAN** est cochée.
7. Sélectionnez **Administrateur** dans le menu déroulant **Droits du niveau du canal**.
8. Saisissez **la clé de cryptage** RMCP+ de votre site, si elle est utilisée.
9. Cliquez sur **Appliquer** si vous avez apporté des modifications dans cet écran.
10. Dans l'arborescence du système, sélectionnez **Système**.
11. Cliquez sur l'onglet **Gestion des alertes**, puis sur **Événements sur plateforme**.

    L'écran **Événements sur plateforme** apparaît, affichant une liste des événements pour lesquels vous pouvez configurer iDRAC6 pour qu'il génère des alertes par e-mail.
12. Activez les alertes par e-mail pour un ou plusieurs événements en cochant la case dans la colonne **Générer des alertes**.
13. Cliquez sur **Appliquer** si vous avez apporté des modifications dans cet écran.
14. Cliquez sur **Paramètres des interruptions**.

    L'écran **Destinations des alertes d'événements sur plateforme** apparaît.
15. Dans le premier champ **Adresse IP de destination** disponible dans la section **Liste des destinations IPv4**, cochez la case **Activé**, puis saisissez l'adresse IP de votre station de gestion.
16. Cliquez sur **Appliquer** si vous avez apporté des modifications dans cet écran.

Vous pouvez maintenant envoyer une interruption test en cliquant sur le lien **Envoyer** dans la colonne **Interruption test**.

Dell vous recommande vivement, à des fins de sécurité, de créer un utilisateur séparé pour les commandes IPMI avec son propre nom d'utilisateur, ses

propres droits IPMI sur le LAN et son propre mot de passe :

1. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ **iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Utilisateurs**.

   L'écran **Utilisateurs** apparaît, affichant une liste de tous les utilisateurs (définis ou non définis).
3. Cliquez sur l'**ID utilisateur** d'un utilisateur non défini.

   L'écran **Configuration de l'utilisateur** pour l'ID utilisateur sélectionné apparaît.
4. Cochez la case **Activer l'utilisateur**, puis saisissez le nom et le mot de passe de l'utilisateur.
5. Dans la section **Droit LAN IPMI**, vérifiez que **Droit maximum de l'utilisateur accordé sur le LAN** est défini sur **Administrateur**.
6. Définissez les autres droits de l'utilisateur selon les besoins.
7. Cliquez sur **Appliquer** pour enregistrer les nouveaux paramètres Utilisateur.

Utilisation d'IT Assistant pour afficher la condition et les événements iDRAC6

Lorsque la découverte est terminée, les périphériques iDRAC6 s'affichent dans la catégorie **Serveurs** de l'écran **Détails des périphériques ITA** et les informations iDRAC6 peuvent être affichées en cliquant sur le nom d'iDRAC6. Ceci diffère des systèmes DRAC5 pour lesquels la carte de gestion apparaît dans le groupe RAC. Ceci est dû au fait qu'iDRAC6 utilise la découverte IPMI par opposition à SNMP.

Les interruptions d'erreurs et d'avertissements iDRAC6 apparaissent désormais dans le **Journal des alertes** principal d'IT Assistant. Elles apparaissent dans la catégorie **Inconnu**, mais la description et la gravité des interruptions seront précises.

Pour plus d'informations sur l'utilisation d'IT Assistant pour la gestion de votre centre de données, veuillez lire le *Guide d'utilisation de Dell OpenManage IT Assistant*.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration de la station de gestion

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

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 les tâches d'installation et de configuration logicielles permettant de configurer une station de gestion afin qu'elle puisse fonctionner avec iDRAC6 Enterprise. Avant de commencer à configurer iDRAC6, suivez les procédures de cette section afin de vous assurer que vous avez installé et configuré les outils dont vous aurez besoin.

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 iDRAC6, 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 iDRAC6, mais non au serveur géré.

Grâce à la fonctionnalité Redirection de console iDRAC6 (consultez la section « Configuration et utilisation des communications série sur le LAN »), 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, par exemple le redémarrage de l'ordinateur, à l'aide des services iDRAC6. 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 pour la configuration des navigateurs Web pris en charge afin de les utiliser avec l'interface Web iDRAC6. Pour une liste des navigateurs Web pris en charge, voir « Navigateurs Web pris en charge ».

Ouverture de votre navigateur Web

L'interface Web iDRAC6 est conçue pour être visualisée dans un navigateur Web pris en charge à une résolution d'écran minimum de 800 pixels (largeur) par 600 pixels (hauteur). Pour visualiser l'interface et accéder à toutes les fonctionnalités, vérifiez que votre résolution est définie sur au moins 800 par 600 pixels et/ou redimensionnez votre navigateur selon les besoins.

REMARQUE : Dans certaines situations, le plus souvent au cours de la première session qui suit une mise à jour du micrologiciel, les utilisateurs d'Internet Explorer 6 peuvent voir apparaître le message **Done, with errors (Terminé, avec des erreurs)** dans la barre d'état du navigateur avec un écran rendu partiellement dans la fenêtre principale du navigateur. Cette erreur peut également se produire si vous rencontrez des problèmes de connectivité. Ce problème est courant avec Internet Explorer 6. Fermez le navigateur et recommencez.

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

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

Pour configurer 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**.

   La fenêtre **Options Internet** s'affiche.
3. Sélectionnez **Outils**→ **Options Internet**→ **Sécurité**→ **Réseau local**.
4. Cliquez sur **Niveau personnalisé**.
5. Sélectionnez **Moyen-Bas** dans le menu déroulant et cliquez sur **Réinitialiser**. Cliquez sur **OK** pour confirmer. Vous devez accéder à nouveau à la boîte de dialogue **Niveau personnalisé** en cliquant sur son bouton.
6. Défilez vers le bas vers la section étiquetée **Contrôles et plug-ins ActiveX** et vérifiez chaque paramètre, car les différentes versions d'IE comportent des paramètres différents dans l'état Moyen-Bas :
   - Invite automatique pour les commandes ActiveX : Activer
   - Comportements binaires et de script : Activer
   - Télécharger les commandes ActiveX signées : Invite
   - Initialiser et mettre sous forme de script les commandes ActiveX qui ne sont pas marquées comme étant sûres : Invite
   - Exécuter les commandes et les plug-in ActiveX : Activer
   - Mettre sous forme de script les commandes ActiveX marquées comme étant sûres pour les scripts : Activer

   Dans la section sur les **Téléchargements** :
   - Invite automatique aux téléchargements de fichiers : Activer
   - Téléchargement de fichiers : Activer
   - Téléchargement de polices : Activer

   Dans la section **Divers** :
   - Autoriser META-REFRESH : Activer
   - Autoriser les scripts de contrôle du navigateur Web Internet Explorer : Activer
   - Autoriser les fenêtres initiées par les scripts sans contraintes de taille ou de position : Activer
   - Ne pas inviter à sélectionner un certificat de client en l'absence de certificats ou lorsqu'il existe un seul certificat : Activer
   - Lancement de programmes et de fichiers dans un IFRAME : Activer
   - Ouvrir des fichiers d'après leur contenu, et non d'après leur extension : Activer
   - Permissions du canal du logiciel : Sécurité basse
   - Soumettre des données non cryptées : Activer
   - Utiliser un bloqueur contextuel : Désactiver

   Dans la section **Scripts** :
   - Script actif : Activer
   - Autoriser les opérations de collage via un script : Activer
   - Scripts des applets Java : Activer

- Sélectionnez **Outils**→ **Options Internet**→ **Avancé**.
- Assurez-vous que les éléments suivants sont cochés ou décochés :

  Dans la section **Navigation** :
  - Toujours envoyer des URL en tant que UTF-8 : coché
  - Désactiver le débogage de scripts (Internet Explorer) : coché
  - Désactiver le débogage de scripts (autre) : coché
  - Afficher une notification à chaque erreur de script : décoché
  - Activer l'installation sur demande (autre) : coché
  - Activer les transitions de pages : coché
  - Activer les extensions de navigateur tierces : coché
  - Réutiliser les fenêtres pour lancer des raccourcis : décoché

Dans la section **Paramètres HTTP 1.1** :

- Utiliser HTTP 1.1 : coché
- Utiliser HTTP 1.1 via des connexions proxy : coché

Dans la section **Java (Sun)** :

- Utiliser JRE 1.6.x_yz : coché (facultatif ; la version peut différer)

Dans la section **Multimédia** :

- Activer le redimensionnement automatique des images : coché
- Lire les animations des pages Web : coché
- Lire les vidéos des pages Web : coché
- Afficher des images : coché

Dans la section **Sécurité** :

- Vérifier la révocation des certificats de l'éditeur : décoché
- Vérifier les signatures des programmes téléchargés : décoché
- Vérifier les signatures des programmes téléchargés : coché
- Utiliser SSL 2.0 : décoché
- Utiliser SSL 3.0 : coché
- Utiliser TLS 1.0 : coché
- Avertir sur les certificats de site invalides : coché
- Avertir en cas de passage du mode sécurisé au mode non sécurisé : coché
- Avertir en cas de redirection de la soumission des formulaires : coché

REMARQUE : Si vous choisissez de modifier l'un des paramètres ci-dessus, Dell vous recommande d'en comprendre les conséquences. Par exemple, si vous choisissez de bloquer les fenêtres contextuelles, des parties de l'interface Web iDRAC6 ne fonctionneront pas correctement.

9. Cliquez sur **Appliquer**, puis sur **OK**.
10. Cliquez sur l'onglet **Connexions**.
11. Sous **Paramètres du réseau local**, cliquez sur **Paramètres réseau**.
12. Si la case **Utiliser un serveur proxy** est cochée, sélectionnez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.
13. Cliquez sur **OK** deux fois.
14. Fermez et redémarrez votre navigateur pour vous assurer que toutes les modifications sont effectives.

Ajout d'iDRAC6 à la liste des domaines de confiance

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

Affichage des versions localisées de l'interface Web

L'interface Web iDRAC6 est prise en charge par les langues suivantes du système d'exploitation :

- Anglais (en-us)
- Français (fr)
- Allemand (de)
- Espagnol (es)
- Japonais (ja)
- Chinois simplifié (zh-cn)

Les identifiants ISO entre parenthèses indiquent les variantes de langue spécifiques qui sont prises en charge. L'utilisation de l'interface avec d'autres dialectes ou langues n'est pas prise en charge et peut ne pas fonctionner comme prévu. Pour certaines langues prises en charge, il pourra être nécessaire de redimensionner la fenêtre du navigateur sur 1 024 pixels (largeur) afin de pouvoir visualiser toutes les fonctionnalités.

L'interface Web iDRAC6 est conçue pour fonctionner avec des claviers localisés pour les variantes de langue spécifiques indiquées ci-dessus. Certaines

fonctionnalités de l'interface Web iDRAC6, comme la redirection de console, peuvent nécessiter des étapes supplémentaires afin de pouvoir accéder à certaines fonctions/lettres. Pour plus de détails sur la manière d'utiliser des claviers localisés dans ces situations, consultez la section « Utilisation du visualiseur vidéo ». L'utilisation d'autres claviers n'est pas prise en charge et peut entraîner des problèmes inattendus.

Internet Explorer 6.0 (Windows)

Pour afficher une version localisée de l'interface Web iDRAC6 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 2.0 (Linux ou Windows)

Pour afficher une version localisée de l'interface Web iDRAC6 dans Firefox 2.0, effectuez les étapes suivantes :

1. Cliquez sur **Outils**→ **Options**, puis sur l'onglet **Avancé**.
2. Sous **Langue**, cliquez sur **Choisir**.

   La fenêtre **Langues** apparaît.
3. Dans le menu déroulant **Sélectionner une langue à ajouter...**, cliquez pour mettre une langue prise en charge en surbrillance, puis cliquez sur **Ajouter**.
4. Cliquez pour sélectionner votre langue préférée, puis cliquez sur **Déplacer vers le haut** jusqu'à ce que la langue apparaisse en haut de la liste.
5. Cliquez sur **OK** pour fermer la fenêtre **Langues**.
6. Cliquez sur **OK** pour fermer la fenêtre **Options**.

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.

Pour définir le jeu de caractères sur un client Linux avec 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 requis. 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 modifications suivantes :

   Entrée actuelle :

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

   Entrée mise à jour :

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

6. Fermez la session puis ouvrez la session sur le système d'exploitation.

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-in pour chaque site distinct hébergeant un plug-in. Si elle est activée, la fonctionnalité Liste blanche vous oblige à installer un visualiseur de redirection de console pour chaque iDRAC6 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 la préférence**, recherchez et double-cliquez sur **xpinstall.whitelist.required**.

   Les valeurs **Nom de la préférence**, **Statut**, **Type** et **Valeur** sont alors affichées en gras. La valeur **Statut** devient **défini par l'utilisateur** et la valeur **Valeur** devient **false**.

4. Dans la colonne **Nom de la préférence**, recherchez **xpinstall.enabled**.

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

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 iDRAC6 avant de lancer le visualiseur. Pour plus d'informations, voir « Configuration de la redirection de console et du média virtuel dans l'interface Web iDRAC6 ».

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 iDRAC6, puis lancée avec 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.

Le programme Java Web Start est automatiquement installé avec JRE ou JDK. Le fichier **jviewer.jnlp** est téléchargé sur votre bureau et une boîte de dialogue vous indique les actions requises à effectuer. Il peut être nécessaire d'associer le type d'extension .jnlp à l'application Java Web Start dans votre navigateur. Sinon, cliquez sur **Ouvrir avec**, puis sélectionnez l'application javaws, qui se trouve dans le sous-répertoire bin de votre répertoire d'installation JRE.

REMARQUE : Si le type de fichier .jnlp n'est pas associé à Java Web Start après l'installation de JRE ou de JDK, vous pouvez définir l'association manuellement. Pour Windows (**javaws.exe**), cliquez sur **Démarrer**→ **Panneau de configuration**→ **Apparence et thèmes**→ **Options des dossiers**. Sous l'onglet **Types de fichiers**, mettez .jnlp en surbrillance sous **Types de fichiers enregistrés**, puis cliquez sur **Modifier**. Pour Linux (**javaws**), lancez Firefox et cliquez sur **Edition**→ **Préférences**→ **Téléchargements**, puis cliquez sur **Voir et modifier les actions**.

Pour Linux, lorsque vous avez installé JRE ou JDK, ajoutez un chemin au répertoire bin Java à l'avant de votre PATH système. Par exemple, si Java est installé dans /usr/java, ajoutez la ligne suivante à votre .bashrc ou /etc/profile local :

```
PATH=/usr/java/bin:$PATH; export PATH
```

REMARQUE : Les fichiers peuvent déjà comporter des lignes de modification du PATH. Vérifiez que les informations de chemin que vous saisissez ne créent pas de conflits.

Installation de clients Telnet ou SSH

Par défaut, le service Telnet iDRAC6 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 iDRAC6. Lorsqu'une connexion est active, toutes les autres tentatives de connexion sont refusées.

Telnet avec iDRAC6

Telnet est inclus dans les systèmes d'exploitation 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 SP1 ou Windows 2003, vous pouvez rencontrer un problème de caractères dans une session Telnet iDRAC6. Ce problème peut se produire sous forme d'ouverture de session gelée où la touche de retour ne répond pas et où l'invite de saisie du mot de passe n'apparaît pas.

Pour résoudre ce problème, téléchargez hotfix 824810 sur le site Web de support de Microsoft à l'adresse **support.microsoft.com**. Consultez l'article 824810 de la Base de connaissances de Microsoft pour plus d'informations.

REMARQUE : Le correctif est nécessaire uniquement pour Windows XP SP1 et Windows 2003. Windows XP SP2 a corrigé le problème.

Configuration de la touche Retour pour les sessions Telnet

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

Pour configurer les clients Telnet Microsoft pour qu'ils utilisent la touche <Retour>, 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.) Retour arrière sera envoyé en tant que 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 iDRAC6

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. iDRAC6 prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé par défaut sur iDRAC6.

Vous pouvez utiliser PuTTY (Windows) ou OpenSSH (Linux) sur une station de gestion pour vous connecter à iDRAC6 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 iDRAC6.

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

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 décrit dans la section « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 Enterprise ».

La mise en uvre SSH iDRAC6 prend en charge plusieurs schémas de cryptographie, comme illustré dans 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 conformément au NIST
Cryptographie symétrique	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Intégrité du message	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentification	• Mot de passe

Installation d'un serveur TFTP

REMARQUE : Si vous utilisez uniquement l'interface Web iDRAC6 pour transférer des certificats SSL et télécharger un nouveau micrologiciel iDRAC6, 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'iDRAC6.

Vous devez uniquement copier des fichiers à destination ou en provenance d'iDRAC6 lorsque vous mettez à jour le micrologiciel iDRAC6 ou installez des certificats sur iDRAC6. 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 iDRAC6 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 logiciel de gestion du système de Dell OpenManage. Ce kit inclut, mais sans limitation, les composants suivants :

- DVD *Dell Systems Management Tools and Documentation*
- 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 *DVD Dell Systems Management Tools and Documentation* 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 du logiciel Dell OpenManage*.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration du serveur géré

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Cette section décrit les tâches permettant de configurer le serveur géré afin d'améliorer vos capacités 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 du dernier plantage.

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 iDRAC6 à partir du serveur 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 du dernier plantage iDRAC6.
- Server Administrator Instrumentation Service : permet d'accéder aux informations détaillées sur les pannes et les performances recueillies par les agents de gestion des systèmes standard de l'industrie 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 la gestion du stockage dans un affichage graphique intégré.
- Journaux de Server Administrator : affiche des journaux de commandes émises vers ou par le système, d'événements matériels surveillés, d'événements POST et d'alertes du système. Vous pouvez afficher les journaux sur la page d'accueil, les imprimer ou les enregistrer comme rapports, puis les envoyer par e-mail à un contact de service désigné.

Utilisez le DVD *Dell Systems Management Tools and Documentation* 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 du dernier plantage

iDRAC6 peut capturer l'écran du dernier plantage afin que vous puissiez l'afficher dans l'interface Web afin de remédier à la cause du plantage du serveur géré. Suivez les étapes ci-dessous pour activer la fonctionnalité Écran du dernier plantage.

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

2. Si vous exécutez Windows, assurez-vous que **Redémarrage automatique** est désélectionné dans **Paramètres de démarrage et de récupération de Windows**. Voir «Désactivation de l'option Redémarrage automatique de Windows».

3. Activez la fonctionnalité **Écran du dernier plantage** (désactivée par défaut) dans l'interface Web iDRAC6.

   Pour activer la fonctionnalité Écran du dernier plantage dans l'interface Web iDRAC6, 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 la fonctionnalité Écran du dernier plantage via la RACADM locale, ouvrez une invite de commande sur le serveur géré et tapez la commande suivante :

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

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

   Pour des informations sur la configuration de l'horloge de **récupération automatique**, consultez le *Guide d'utilisation de Server Administrator*. Pour que l'écran du dernier plantage soit capturé, l'**horloge de récupération automatique** doit être définie sur 60 secondes. Le paramètre 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 Redémarrage automatique de Windows

Pour s'assurer qu'iDRAC6 peut capturer l'écran du dernier plantage, désactivez l'option **Redémarrage automatique** sur les serveurs gérés exécutant 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. Décochez la case **Redémarrage automatique**.
5. Cliquez sur **OK** deux fois.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration d'iDRAC6 Enterprise via l'interface Web

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

iDRAC6 intègre une interface Web qui vous permet de configurer les propriétés et les utilisateurs iDRAC6, 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 iDRAC6. Ce chapitre décrit comment effectuer les tâches de gestion de systèmes courantes en utilisant l'interface Web iDRAC6 et 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 d'iDRAC6 Enterprise ».

Accès à l'interface Web

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

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

   Pour plus d'informations, voir «Navigateurs Web pris en charge».

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 iDRAC6 et *numéro de port,* le numéro de port HTTPS.

   La fenêtre **Ouverture de session** iDRAC6 apparaît.

Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur iDRAC6 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 iDRAC6.

Pour ouvrir une session, effectuez les étapes suivantes.

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

   - Votre nom d'utilisateur iDRAC6.

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

   - Votre nom d'utilisateur Active Directory.

     Pour les noms Active Directory, vous pouvez utiliser n'importe lequel des formats suivants : *<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`. À défaut, vous pouvez indiquer le domaine dans le champ **Domaine**.

2. Dans le champ **Mot de passe**, tapez votre mot de passe utilisateur iDRAC6 ou Active Directory. La différence entre majuscules et minuscules est prise en compte.

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.

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

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

REMARQUE : La fermeture de l'interface Web iDRAC6 dans 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**.

Utilisation des multiples onglets et fenêtres du navigateur

Les diverses versions des navigateurs Web impliquent des comportements différents à l'ouverture de nouveaux onglets et fenêtres. Chaque fenêtre correspond à une nouvelle session, contrairement à chaque nouvel onglet. Microsoft Internet Explorer 6 ne prend pas en charge les onglets ; par conséquent, chaque fenêtre ouverte du navigateur devient une nouvelle session de l'interface Web iDRAC6. Internet Explorer 7 possède l'option permettant d'ouvrir les onglets ainsi que les fenêtres. Chaque onglet hérite des caractéristiques du dernier onglet ouvert. Par exemple, si un utilisateur ouvre une session avec des privilèges d'utilisateur privilégié sur un onglet, puis qu'il ouvre une session en tant qu'administrateur sur un autre onglet, les deux onglets ouverts possèdent alors des privilèges d'administrateur. La fermeture d'un onglet, quel qu'il soit, fait expirer tous les onglets de l'interface Web iDRAC6.

Le comportement des onglets dans Firefox 2 est le même que dans Internet Explorer 7 ; les nouveaux onglets initient de nouvelles sessions. Le comportement des fenêtres dans Firefox est toutefois différent. Les fenêtres de Firefox fonctionnent avec les mêmes privilèges que la dernière fenêtre ouverte. Par exemple, si une seule fenêtre Firefox est ouverte avec un utilisateur privilégié ayant ouvert une session et qu'une autre fenêtre est ouverte avec des privilèges d'administrateur, **les deux** utilisateurs auront maintenant des privilèges d'administrateur.

Tableau 5-1. Comportement des privilèges utilisateur dans les navigateurs pris en charge

Navigateur	Comportement des onglets	Comportement des fenêtres
Microsoft Internet Explorer 6	Non applicable	Nouvelle session
Microsoft Internet Explorer 7	Depuis la dernière session ouverte	Nouvelle session
Firefox 2	Depuis la dernière session ouverte	Depuis la dernière session ouverte

---

Configuration du NIC iDRAC6

Cette section suppose qu'iDRAC6 a déjà été configuré et est accessible sur le réseau. Voir « Configurer la mise en réseau iDRAC6 » pour obtenir de l'aide sur la configuration réseau iDRAC6 initiale.

Configuration des paramètres du réseau et du LAN IPMI

REMARQUE : Vous devez disposer du privilège de **configuration iDRAC6** pour effectuer les étapes suivantes.

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

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

2. Cliquez sur l'onglet **Réseau/Sécurité**.

   L'écran **Configuration réseau** s'affiche.

3. Configurez les paramètres du réseau et du réseau local IPMI selon vos besoins. Voir Tableau 5-2 et Tableau 5-3 pour des descriptions des options **Paramètres réseau** et **Paramètres LAN IPMI**.

4. Cliquez sur **Appliquer**.

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

Tableau 5-2. 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 iDRAC6 via le réseau sont bloquées. La valeur par défaut est **Désactivé**.

MAC Address (Adresse Mac)	Affiche l'adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nud d'un réseau. L'adresse MAC ne peut pas être modifiée.
Utiliser DHCP (pour l'adresse IP du NIC)	Demande à iDRAC6 d'obtenir une adresse IP pour le NIC sur le serveur de protocole de configuration dynamique des hôtes (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'iDRAC6. 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'iDRAC6. 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'iDRAC6. 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 préféré statique	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 iDRAC6 sur le serveur DNS. La valeur par défaut est **Désactivé**.
iDRAC DNS Nom	Affiche le nom iDRAC6 uniquement lorsque l'option **Enregistrer iDRAC sur DNS** est sélectionnée. Le nom par défaut est idrac-*numéro_de_service*, où *numéro_de_service* est le numéro de service du serveur Dell. Par exemple : idrac-00002.
Utiliser DHCP pour le nom de domaine DNS	Utilise le nom de domaine DNS par défaut. Si la case n'est pas cochée et que l'option **Enregistrer iDRAC sur DNS** est sélectionnée, changez le nom de domaine DNS dans le champ **Nom de domaine DNS**. La valeur par défaut est **Désactivé**. **REMARQUE :** Pour cocher la case **Utiliser DHCP pour le nom de domaine DNS**, cochez également la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Nom de domaine DNS	Le champ du **nom de domaine DNS** par défaut est vide. Lorsque la case **Utiliser DHCP pour le nom de domaine DNS** est cochée, cette option est grisée et le champ ne peut pas être modifié.

Tableau 5-3. Paramètres LAN IPMI

Paramètre	Description
Activer IPMI sur le réseau local	Lorsque ce paramètre est coché, indique que le canal LAN IPMI est activé. La valeur par défaut est **Désactivé**.
Limite du niveau de privilège du canal	Configure le niveau de privilège 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 espace autorisé). Par défaut, aucune valeur n'est indiquée.

Tableau 5-4. Boutons de configuration réseau

Bouton	Description
Paramètres avancés	Ouvre l'écran **Sécurité réseau** pour permettre à l'utilisateur d'entrer les valeurs de la plage IP et les attributs de blocage IP.
Imprimer	Imprime les valeurs de **Configuration réseau** qui apparaissent à l'écran.
Actualiser	Recharge l'écran **Configuration réseau**.
Appliquer	Enregistre les nouveaux paramètres définis sur l'écran Configuration réseau. **REMARQUE :** La modification des paramètres de l'adresse IP du NIC entraîne la fermeture de toutes les sessions utilisateur et force les utilisateurs à se reconnecter à l'interface Web d'iDRAC6 avec les paramètres d'adresse IP mis à jour. Toutes les autres modifications nécessitent la réinitialisation du NIC, qui peut provoquer une perte brève de connectivité.

Configuration du filtrage IP et du blocage IP

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

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

   L'écran **Configuration réseau** s'affiche.
3. Cliquez sur **Paramètres avancés**.

   L'écran **Sécurité réseau** s'affiche.
4. Configurez les paramètres de blocage et de filtrage IP selon vos besoins. Voir Tableau 5-5 pour des descriptions des paramètres de **blocage et filtrage IP**.
5. Cliquez sur **Appliquer**.
6. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-6.

Tableau 5-5. Paramètres de la 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 iDRAC6. La valeur par défaut est **Désactivé**.
Adresse de la plage IP	Détermine l'adresse de sous-réseau IP acceptée. L'adresse par défaut est **192.168.1.0**.
Masque de sous-réseau de la plage IP	Définit les positions des bits de fort poids dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau, où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur. L'adresse par défaut est **255.255.255.0**.
Blocage IP activé	Active la fonctionnalité de blocage d'adresse IP, qui limite le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP spécifique pendant une durée prédéfinie. La valeur par défaut est **Désactivé**.
Nombre d'échecs avant blocage IP	Définit le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP avant de rejeter les tentatives d'ouverture de session à partir de cette adresse. L'adresse par défaut est **10**.
Plage d'échecs avant blocage IP	Détermine la période en secondes pendant laquelle doivent se produire des échecs du nombre d'échecs avant blocage IP pour déclencher la période de pénalité avant blocage IP. L'adresse par défaut est **3600**.
Période de pénalité avant blocage IP	Période, en secondes, pendant laquelle les tentatives d'ouverture de session à partir d'une adresse IP avec un nombre d'échecs excessif sont rejetées. L'adresse par défaut est **3600.**

Tableau 5-6. Boutons de la sécurité réseau

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

Configuration des événements sur plateforme

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

Les événements sur plateforme filtrables sont répertoriés dans Tableau 5-7.

Tableau 5-7. Événements sur plateforme filtrables

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 vos 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 iDRAC6.
2. Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.

   L'écran **Événements sur plateforme** s'affiche.
3. Sélectionnez la case à cocher **Génération d'une alerte** en regard de chacun des événements pour lesquels vous souhaitez qu'une alerte soit déclenchée.

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

4. Sélectionnez le bouton radio sous l'action que vous voulez activer pour chaque événement. Vous ne pouvez sélectionner qu'une action pour chacun des événements.
5. Cliquez sur **Appliquer**.

REMARQUE : **Générer une alerte** doit être activé pour qu'une alerte soit envoyée à une destination configurée valide (PET ou 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 à l'interface Web iDRAC6.
2. Assurez-vous d'avoir bien suivi les procédures dans « Configuration des filtres d'événements sur plateforme (PEF) ».
3. Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.

   L'écran **Événements sur plateforme** s'affiche.
4. Cliquez sur **Paramètres des interruptions**.

   L'écran **Destinations des alertes d'événements sur plateforme** s'affiche.
5. Configurez votre adresse IP de destination PET.
   a. Sélectionnez la case à cocher **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 iDRAC6.

   c. Cliquez sur **Appliquer**.

   REMARQUE : Pour un envoi réussi d'une interruption, configurez la valeur de la **chaîne de communauté** sur l'écran **Configuration réseau**. La valeur **Chaîne de communauté** indique la chaîne de communauté à utiliser dans une interruption d'alerte SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]) envoyée à partir d'iDRAC6. Les interruptions d'alerte SNMP sont transmises par iDRAC6 quand un événement sur plateforme se produit. Le paramètre par défaut pour la **chaîne de communauté** est **Public**.

d. Pour tester l'alerte configurée, cliquez sur **Envoyer**.

e. Pour ajouter une autre adresse IP de destination, recommencez la procédure décrite de l'étape a à l'étape d. Vous pouvez indiquer jusqu'à quatre adresses IP de destination.

Configuration des alertes par e-mail

1. Connectez-vous à l'interface Web iDRAC6.
2. Assurez-vous d'avoir bien suivi les procédures dans « Configuration des filtres d'événements sur plateforme (PEF) ».
3. Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.

   L'écran **Événements sur plateforme** s'affiche.
4. Cliquez sur **Paramètres d'alertes par e-mail**.

   L'écran correspondant s'affiche.
5. Configurez votre destination d'alerte par e-mail.
   a. Sélectionnez la case à cocher **Activé** pour la première alerte par e-mail non définie.
   b. Entrez une adresse e-mail valide dans le champ **Adresse e-mail de destination**.
   c. Cliquez sur **Appliquer**.

   REMARQUE : Pour réussir à envoyer un e-mail test, l'**adresse du serveur SMTP** doit être configurée dans la section relative aux **paramètres de l'adresse du serveur SMTP (e-mail)** dans l'écran **Paramètres d'alertes par e-mail**. L'adresse IP du **serveur SMTP** communique avec iDRAC6 pour envoyer des alertes par e-mail lorsqu'un événement sur plateforme se produit.

   d. Cliquez sur **Envoyer** pour tester l'alerte par e-mail configurée (si nécessaire).
   e. Pour ajouter une autre destination d'alerte par e-mail, recommencez la procédure décrite de l'étape a à l'étape d. Vous pouvez indiquer jusqu'à quatre destinations d'alerte par e-mail.

Configuration d'IPMI sur le LAN

1. Connectez-vous à l'interface Web iDRAC6.
2. Configurez IPMI sur le réseau local LAN.
   a. Cliquez sur **Système→ Accès à distance→ iDRAC**, puis cliquez sur l'onglet **Réseau/Sécurité**.

      L'écran **Configuration réseau** s'affiche.
   b. Cliquez sur **Paramètres LAN IPMI**.
   c. Sélectionnez la case à cocher **Activer IPMI sur le LAN**.
   d. Mettez à jour les privilèges de canal LAN IPMI, si nécessaire.

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

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

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

   REMARQUE : L'interface IPMI iDRAC6 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**, indiquez la clé de cryptage.

   f. Cliquez sur **Appliquer**.
3. Configurez Communications série IPMI sur le LAN (SOL).
   a. Cliquez sur **Système→ Accès à distance→ iDRAC**, puis cliquez sur l'onglet **Réseau/Sécurité**.

      L'écran **Configuration réseau** s'affiche.
   b. Accédez à l'écran **Communications série sur le LAN**.

c. Sélectionnez la case à cocher **Activation des communications série sur le LAN**.

d. Si nécessaire, mettez à jour le débit en bauds SOL IPMI en sélectionnant une vitesse de données dans le menu déroulant Débit en bauds.

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.

e. Cliquez sur **Appliquer**.

Ajout et configuration des utilisateurs iDRAC6

Pour gérer votre système avec iDRAC6 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 iDRAC6, effectuez les étapes suivantes :

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

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

2. Ouvrez l'écran **Utilisateurs** pour configurer des utilisateurs.

   L'écran **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 **ID d'utilisateur**, cliquez sur un ID d'utilisateur.

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

   Tableau 5-8 décrit les paramètres **généraux** pour configurer un nom d'utilisateur et un mot de passe iDRAC6.

   Tableau 5-9 décrit les **Privilèges d'utilisateur IPMI** pour la configuration des privilèges LAN de l'utilisateur.

   Tableau 5-10 décrit les droits du **groupe d'utilisateurs** pour les paramètres **Privilèges d'utilisateur IPMI** et Privilèges d'utilisateur iDRAC.

   Tableau 5-11 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 5-12.

Tableau 5-8. Propriétés générales

Propriété	Description
ID d'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 iDRAC6 est activé. Lorsqu'elle est décochée, l'accès utilisateur est désactivé.
Le nom d'utilisateur	Spécifie un nom d'utilisateur iDRAC6 contenant jusqu'à 16 caractères. Chaque utilisateur doit avoir un nom d'utilisateur unique. **REMARQUE :** Les noms d'utilisateur iDRAC6 ne peuvent pas comporter les caractères **/** (barre oblique) ou **.** (point). **REMARQUE :** Si le nom d'utilisateur est modifié, le nouveau nom n'apparaît pas dans l'interface utilisateur jusqu'à la prochaine ouverture de session utilisateur.
Modifier le mot de passe	Active les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. Lorsque cette option n'est pas sélectionnée, le **mot de passe** de l'utilisateur ne peut pas être modifié.
Nouveau mot de passe	Active la modification du mot de passe de l'utilisateur iDRAC6. Entrez un **mot de passe** de 20 caractères au maximum. Les caractères ne seront pas affichés.
Confirmer le nouveau mot de passe	Indiquez de nouveau le mot de passe de l'utilisateur iDRAC6 pour le confirmer.

Tableau 5-9. Privilèges utilisateur sur le LAN IPMI

Propriété	Description
Privilège maximum de l'utilisateur accordé sur le LAN	Spécifie le privilège maximal de l'utilisateur sur le canal LAN IPMI sur l'un des groupes d'utilisateurs suivants : **Aucun**, **Administrateur**, **Opérateur** ou **Utilisateur**.
Activer la connexion série sur le réseau local	Permet à l'utilisateur d'utiliser les communications série sur le LAN IPMI. Lorsque cette option est sélectionnée, ce privilège est activé.

Tableau 5-10. Privilèges utilisateur iDRAC6

Propriété	Description
Groupe iDRAC	Spécifie le privilège utilisateur iDRAC6 maximal sur un des groupes d'utilisateurs suivants : **Administrateur**, **Utilisateur privilégié**, **Utilisateur invité**, **Personnalisé** ou **Aucun**. Voir Tableau 5-11 pour connaître les droits **Groupe iDRAC6**.
Ouvrir une session iDRAC	Permet à l'utilisateur d'ouvrir une session iDRAC6.
Configurer iDRAC	Permet à l'utilisateur de configurer iDRAC6.
Configurer les utilisateurs	Permet à l'utilisateur de permettre à des utilisateurs spécifiques d'accéder au système.
Effacer les journaux	Permet à l'utilisateur d'effacer les journaux iDRAC6.
Exécuter les commandes de contrôle du serveur	Permet à l'utilisateur d'exécuter des commandes RACADM.
Accéder à la redirection de console	Permet à l'utilisateur d'exécuter la redirection de console.
Accéder au média virtuel	Permet à l'utilisateur d'exécuter et d'utiliser le média virtuel.
Tester les alertes	Permet à l'utilisateur d'envoyer des alertes de test (e-mail et PET) à un utilisateur spécifique.
Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Tableau 5-11. Droits Groupe iDRAC6

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**
None (Aucun)	Aucun droit attribué

Tableau 5-12. Boutons pour la configuration utilisateur

Bouton	Action
Imprimer	Imprime les valeurs de **Configuration utilisateur** qui apparaissent à l'écran.
Actualiser	Recharge l'écran **Configuration utilisateur**.
Appliquer	Enregistre les nouveaux paramètres définis pour la configuration utilisateur.
Retour à l'écran Utilisateurs	Retourne à l'**écran Utilisateurs**.

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

Cette section fournit des informations sur les fonctionnalités de sécurité des données intégrées à iDRAC6 :

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

Secure Sockets Layer (SSL)

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

Un système compatible SSL peut effectuer les tâches suivantes :

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

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

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

Requête de signature de certificat (RSC)

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

Une fois que l'autorité de certification approuve la RSC et qu'elle envoie le certificat, téléchargez ce dernier sur le micrologiciel iDRAC6. Les informations de la RSC enregistrées sur le micrologiciel iDRAC6 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 l'écran **Menu principal SSL**.

Utilisez l'écran **Menu principal SSL** pour générer une RSC à envoyer à une autorité de certification. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6.

Tableau 5-13 décrit les options disponibles lors de la génération d'une RSC.

Tableau 5-14 décrit les boutons disponibles sur l'écran **Menu principal SSL**.

Tableau 5-13. Options du menu principal SSL

Champ	Description
Générer une nouvelle requête de signature de certificat (RSC)	Sélectionnez l'option et cliquez sur **Suivant** pour ouvrir l'écran **Générer une requête de signature de certificat (RSC)**. **REMARQUE :** Chaque nouvelle RSC supplante la RSC qui se trouve déjà sur le micrologiciel. Pour qu'une CA accepte votre RSC, la RSC du micrologiciel doit correspondre au certificat renvoyé par la CA.
Télécharger le certificat de serveur	Sélectionnez l'option et cliquez sur **Suivant** pour ouvrir l'écran **Téléchargement d'un certificat**. Téléchargez ensuite le certificat que l'autorité de certification vous a envoyé. **REMARQUE :** iDRAC6 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 l'écran **Afficher le certificat de serveur** et afficher un certificat de serveur existant.

Tableau 5-14. Boutons du menu principal SSL

Bouton	Description
Imprimer	Imprime les valeurs de **Menu principal SSL** qui apparaissent à l'écran.
Actualiser	Recharge l'écran **Menu principal SSL**.

Suivant	Traite les informations de l'écran **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. Dans le cas contraire, iDRAC6 n'acceptera pas le certificat.

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

   Tableau 5-15 décrit les options de l'écran **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 5-16.

Tableau 5-15. Options de génération d'une requête de signature de certificat (RSC)

Champ	Description
Nom commun	Le nom exact à certifier (normalement, le nom de domaine du serveur Web, par exemple, **www.compagniexyz.com**). Seuls les caractères alphanumériques, les tirets, les traits de soulignement et les points sont valides. Les espaces ne sont pas valides.
Nom de la société	Le nom associé à cette société (par exemple, Compagnie XYZ). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Service de la société	Nom associé au service, comme un département (par exemple, Informatique). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Ville	La ville ou tout autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Seuls les caractères alphanumériques et les espaces sont valides. Ne séparez pas les mots par des traits de soulignement ou d'autres caractères.
Nom de l'état	L'état ou la province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Seuls les caractères alphanumériques et les espaces sont valides. N'utilisez pas d'abréviations.
Code du pays	Le nom du pays où se trouve l'entité qui fait la demande de certification.
E-mail	L'adresse e-mail associée à la RSC. Tapez l'adresse e-mail de l'entreprise ou toute autre adresse e-mail associée à la RSC. Ce champ est optionnel.

Tableau 5-16. Boutons de génération d'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 l'écran **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 l'écran **Menu principal SSL**.

Téléchargement d'un certificat de serveur

1. Sur l'écran **Menu principal SSL**, sélectionnez **Télécharger le certificat de serveur** et cliquez sur **Suivant**.

   L'écran **Téléchargement 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 du certificat que vous téléchargez. Vous devez entrer le chemin, y compris le chemin et le nom de fichier complets et l'extension du fichier.

3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-17.

Tableau 5-17. Boutons de téléchargement d'un certificat

Bouton	Description
Imprimer	Imprime les valeurs qui apparaissent sur l'écran **Téléchargement d'un certificat**.
Actualiser	Recharge l'écran **Téléchargement d'un certificat**.
Appliquer	Applique le certificat au micrologiciel iDRAC6.
Retour au menu principal SSL	Renvoie l'utilisateur à l'écran **Menu principal SSL**.

Affichage d'un certificat de serveur

1. Sur l'écran **Menu principal SSL**, sélectionnez **Afficher le certificat de serveur** et cliquez sur **Suivant**.

   Tableau 5-18 décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

2. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-19.

Tableau 5-18. Informations relatives au certificat

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

Tableau 5-19. Boutons pour l'affichage du certificat de serveur

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

Configuration et gestion des certificats Active Directory

REMARQUE : Vous devez avoir le droit de **configurer iDRAC** pour configurer Active Directory, 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'iDRAC6 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 l'écran **Menu principal d'Active Directory**.

   Tableau 5-20 répertorie les options dans **Menu principal d'Active Directory**.

3. Cliquez sur le bouton approprié pour continuer. Voir tableau 5-20.

   Tableau 5-20. Options du 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**.
Télécharger le certificat CA d'Active Directory	Télécharge un certificat Active Directory sur iDRAC6.
Afficher le certificat CA d'Active Directory	Affiche un certificat Active Directory qui a été téléchargé sur iDRAC6.

Tableau 5-21. Boutons du menu principal d'Active Directory

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

Configuration d'Active Directory (schéma standard et schéma étendu)

1. Sur l'écran **Menu principal d'Active Directory**, sélectionnez **Configurer Active Directory** et cliquez sur **Suivant**.
2. Sur l'écran **Configuration d'Active Directory**, entrez les paramètres Active Directory.

   Tableau 5-22 décrit les paramètres de **Configuration et gestion d'Active Directory**.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.
4. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-23.
5. Pour configurer les groupes de rôles pour le schéma standard d'Active Directory, cliquez sur le groupe de rôles individuel (1-5). Reportez-vous à la Tableau 5-24et à la section Tableau 5-25.

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

Tableau 5-22. Paramètres de configuration d'Active Directory

Paramètre	Description
Activer Active Directory	Lorsqu'il est coché, active Active Directory. **Désactivé** est sélectionné par défaut.
Nom de domaine ROOT	Nom de domaine ROOT d'Active Directory. Par défaut, aucune valeur n'est indiquée. 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. Par défaut, aucune valeur n'est indiquée.
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 étendu	Utilise le schéma étendu avec Active Directory.
Nom iDRAC	Nom qui identifie de manière exclusive iDRAC6 dans Active Directory. Par défaut, aucune valeur n'est indiquée. 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 iDRAC6 réside. Par défaut, aucune valeur n'est indiquée. 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.
Groupes de rôles	Liste des groupes de rôles associés à iDRAC6. Pour modifier les paramètres d'un groupe de rôles, cliquez sur le numéro du groupe de rôles dans la liste des groupes de rôles.
Nom du groupe	Nom qui identifie le groupe de rôles d'Active Directory associé à iDRAC6. Par défaut, aucune valeur n'est indiquée.
Domaine du groupe	Type de domaine où le groupe de rôles réside.

Tableau 5-23. Boutons de configuration d'Active Directory

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

Tableau 5-24. Privilèges du groupe de rôles

Paramètre	Description
Niveau de privilège du groupe de rôles	Spécifie le privilège utilisateur iDRAC6 maximum sur un des groupes d'utilisateurs suivants : **Administrateur**, **Utilisateur privilégié**, **Utilisateur invité**, **Aucun** ou **Personnalisé**. Voir Tableau 5-25 pour connaître les droits **Groupe de rôles**.
Ouvrir une session iDRAC	Permet au groupe d'ouvrir une session pour accéder à iDRAC6.
Configurer iDRAC	Permet au groupe de configurer iDRAC6.
Configurer les utilisateurs	Permet au groupe de configurer des utilisateurs.
Effacer les journaux	Permet au groupe d'effacer des journaux.
Exécuter les commandes de contrôle du serveur	Permet au groupe d'exécuter des commandes de contrôles du serveur.
Accéder à la redirection de console	Permet au groupe d'accéder à la redirection de console.
Accéder 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.
Exécuter des commandes de diagnostic	Permet au groupe d'exécuter des commandes de diagnostics.

Tableau 5-25. Droits du groupe 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**
None (Aucun)	Aucun droit attribué

Téléchargement d'un certificat CA d'Active Directory

1. Sur l'écran **Menu principal d'Active Directory**, sélectionnez **Télécharger le certificat d'autorité de certification d'Active Directory** et cliquez sur **Suivant**.

2. Sur l'**écran Téléchargement d'un certificat,** dans le champ **Chemin d'accès au fichier**, tapez le chemin d'accès au fichier du certificat ou cliquez sur **Parcourir** pour accéder au fichier de certificat.

REMARQUE : La valeur **Chemin d'accès au fichier** affiche le chemin du certificat que vous téléchargez. Vous devez entrer le chemin, y compris le chemin et le nom de fichier complets et 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 iDRAC6.

3. Cliquez sur **Appliquer**.

4. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-26.

Tableau 5-26. Boutons de téléchargement d'un certificat

Bouton	Description
Imprimer	Imprime les valeurs de **Téléchargement d'un certificat** apparaissant à l'écran.
Actualiser	Recharge l'écran **Téléchargement d'un certificat**.
Appliquer	Applique le certificat au micrologiciel iDRAC6.
Retourner à la page Menu principal d'Active Directory	Retourne à l'écran **Menu principal d'Active Directory**.

Affichage d'un certificat CA d'Active Directory

Utilisez l'écran **Menu principal d'Active Directory** pour afficher un certificat de serveur d'autorité de certification pour votre iDRAC6.

1. Sur l'écran **Menu principal d'Active Directory**, sélectionnez **Télécharger le certificat d'autorité de certification d'Active Directory** et cliquez sur **Suivant**.

   Tableau 5-27 décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

2. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-28.

Tableau 5-27. Informations relatives au certificat CA d'Active Directory

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

Tableau 5-28. Boutons d'affichage du 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 l'**écran Certificat d'autorité de certification d'Active Directory**.
Retourner à la page Menu principal d'Active Directory	Renvoie l'utilisateur à l'écran **Menu principal d'Active Directory**.

Activation ou désactivation de l'accès à la configuration locale

REMARQUE : Le paramètre par défaut de l'accès à la configuration locale est **Activé**.

Activation de l'accès à la configuration locale

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**.
2. Sous **Configuration locale**, cliquez pour décocher **Désactiver les mises à jour de la configuration UTILISATEUR locale iDRAC** pour activer l'accès.
3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-34.

Désactivation de l'accès à la configuration locale

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**.
2. Sous **Configuration locale**, cliquez pour cocher **Désactiver les mises à jour de la configuration UTILISATEUR locale iDRAC** pour désactiver l'accès.
3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Voir Tableau 5-34.

Configuration des services iDRAC6

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.

REMARQUE : Il existe un problème connu avec le client Telnet fourni avec Microsoft Windows communicant avec un BMU. Utilisez un autre client Telnet tel que HyperTerminal ou PuTTY.

1. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis cliquez sur l'onglet **Réseau/Sécurité**.
2. Cliquez sur **Services** pour ouvrir l'écran de configuration **Services**.
3. Configurez les services suivants, si nécessaire :
   - Web Server : voir Tableau 5-29 pour accéder aux paramètres Web Server
   - SSH : voir Tableau 5-30 pour accéder aux paramètres SSH
   - Telnet : voir Tableau 5-31 pour accéder aux paramètres telnet
   - Agent SNMP : voir Tableau 5-32 pour accéder aux paramètres de l'agent SNMP
   - Agent de récupération automatique du système : voir Tableau 5-33 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 5-34.

Tableau 5-29. Paramètres de Web Server

Paramètre	Description
Activé	Active ou désactive le serveur Web iDRAC6. Lorsqu'elle est cochée, cette case indique que Web Server est activé. Par défaut, il est **activé**.
Nombre maximal de sessions	Nombre maximal 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 au **Nombre maximal de sessions**. Ce champ ne peut pas être modifié.
Délai d'attente	Durée, en secondes, pendant laquelle une connexion peut rester inactive. La session est annulée quand le délai d'expiration est atteint. Les modifications apportées au paramètre de délai d'attente prennent effet immédiatement et réinitialisent Web Server. La plage du délai d'expiration est comprise entre 60 et 10 800 secondes. La valeur par défaut est **1 800** secondes.
Numéro de port HTTP	Port sur lequel iDRAC6 écoute une connexion au navigateur. L'adresse par défaut est **80**.
Numéro de port HTTPS	Port sur lequel iDRAC6 écoute une connexion sécurisée au navigateur. L'adresse par défaut est **443**.

Tableau 5-30. 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 maximal 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'expiration est comprise entre 60 et 10 800 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La valeur par défaut est **1 800**.
Numéro de port	Port sur lequel iDRAC6 écoute une connexion SSH. L'adresse par défaut est **22**.

Tableau 5-31. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé. Par défaut, il est **désactivé**.
Nombre maximal de sessions	Nombre maximal 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'expiration est comprise entre 60 et 10 800 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La valeur par défaut est **1 800**.
Numéro de port	Port sur lequel iDRAC6 écoute une connexion Telnet. L'adresse par défaut est **23**.

Tableau 5-32. Agent SNMP

Paramètre	Description
Activé	Active ou désactive les alertes par e-mail.
Nom de communauté SNMP	Nom de communauté qui contient l'adresse IP pour la destination de l'alerte SNMP. Le nom de communauté peut comporter jusqu'à 31 caractères (sans espace). La valeur par défaut est « public ».

Tableau 5-33. Paramètre de l'agent de récupération de système automatique

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

Tableau 5-34. Boutons pour les services

Bouton	Description
Imprimer	Imprime l'écran **Services**.
Actualiser	Actualise l'écran **Services**.
Appliquer les modifications	Applique les paramètres de l'écran **Services**.

Mise à jour du micrologiciel iDRAC6

REMARQUE : Si le micrologiciel iDRAC6 devient corrompu, ce qui peut être le cas lorsque la progression de la mise à jour du micrologiciel iDRAC6 est interrompue avant qu'elle ne se termine, vous pouvez récupérer iDRAC6 à l'aide de 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 iDRAC6 définis. Lors du processus de mise à jour, vous avez la possibilité de rétablir les paramètres d'usine de la configuration iDRAC6. 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 iDRAC6 ou via l'interface Web CMC.

1. Démarrez l'interface Web iDRAC6.
2. Cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis cliquez sur l'onglet **Mise à jour**.

   REMARQUE : Pour mettre à jour le micrologiciel, iDRAC6 doit être en mode de mise à jour. Dans ce mode, iDRAC6 se réinitialise automatiquement, même si vous annulez le processus de mise à jour.

3. Sur l'écran **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 : Téléchargement (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\V2.0\<nom_de_l'image>`.

   Par défaut, le nom de l'image du micrologiciel est **firmimg.imc**.

5. Cliquez sur **Suivant**.
   - Le fichier va se télécharger sur iDRAC6. This may take several minutes to complete.

     OU

   - Cliquez sur **Annuler** à cet instant pour arrêter le processus de mise à niveau du micrologiciel. Si vous cliquez sur **Annuler,** iDRAC6 revient au mode de fonctionnement normal.

- 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 téléchargé.
  - Si le fichier image s'est téléchargé 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 téléchargée ou n'a pas réussi les vérifications, la mise à jour de micrologiciel retourne à la fenêtre **Mise à jour de micrologiciel : Téléchargement (page 1 sur 4)**. Vous pouvez réessayer de mettre à niveau iDRAC6 ou cliquer sur **Annuler** pour qu'iDRAC6 revienne à son mode de fonctionnement normal.

REMARQUE : Si vous décochez la case **Préserver la configuration**, les paramètres par défaut d'iDRAC6 seront rétablis. Dans les paramètres par défaut, le LAN est désactivé. Vous ne pourrez pas vous connecter à l'interface Web iDRAC6. Vous devrez reconfigurer les paramètres LAN via l'interface Web CMC ou iKVM à l'aide de l'utilitaire de configuration iDRAC6 lors du POST du BIOS.

7. Par défaut, la case **Préserver la configuration** est cochée pour conserver les paramètres iDRAC6 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 du micrologiciel terminée, la fenêtre **Mise à jour de micrologiciel : Résultats de la mise à jour (page 4 sur 4)** apparaît et iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC6 avec une nouvelle fenêtre de navigateur.

Mise à jour du micrologiciel iDRAC6 à l'aide de CMC

Généralement, le micrologiciel iDRAC6 est mis à jour à l'aide des services iDRAC6, comme par exemple l'interface Web iDRAC6 ou les progiciels de mise à jour spécifiques au système d'exploitation téléchargés à l'adresse **support.dell.com**.

Vous pouvez utiliser l'interface Web CMC ou les commandes RACADM CMC pour mettre à jour le micrologiciel iDRAC6. Cette fonctionnalité est disponible que le micrologiciel iDRAC6 soit en mode normal ou corrompu. Voir « Mise à jour du micrologiciel iDRAC6 à l'aide de 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 iDRAC6, effectuez les étapes suivantes :

1. Téléchargez la dernière version du micrologiciel iDRAC6 sur votre ordinateur de gestion depuis l'adresse **support.dell.com**.

2. Connectez-vous à l'interface Web du module CMC.

3. Sélectionnez **Chassis** (Châssis) **dans l'arborescence**.

4. Cliquez sur l'onglet **Update** (Mise à jour). L'écran **Updatable Components** (Composants actualisables) s'affiche.

5. Cliquez sur **serveur-*n***, où ***n*** est le numéro du serveur pour lequel vous souhaitez mettre à jour iDRAC6.

6. Cliquez sur **Parcourir,** localisez l'image du micrologiciel iDRAC6 que vous avez téléchargée et cliquez sur **Ouvrir**.

7. Cliquez sur **Commencer la mise à jour de micrologiciel**.

Une fois le fichier image téléchargé sur CMC, iDRAC6 se met à jour avec l'image.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation d'iDRAC6 avec Microsoft Active Directory

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Un service de répertoire permet de maintenir une base de données commune rassemblant toutes les informations nécessaires au contrôle des utilisateurs, des ordinateurs, des imprimantes, etc. d'un réseau. Si votre société utilise déjà le logiciel de service Microsoft® Active Directory®, celui-ci peut être configuré pour vous donner accès à iDRAC6 et vous permettre d'ajouter et de contrôler les privilèges utilisateur iDRAC6 pour les utilisateurs présents dans votre logiciel Active Directory.

REMARQUE : L'utilisation d'Active Directory pour reconnaître les utilisateurs d'iDRAC6 est prise en charge sur les systèmes d'exploitation Microsoft Windows 2000, Windows Server 2003 et Windows Server 2008.

La table Tableau 6-1 affiche les neuf privilèges des utilisateurs iDRAC6 dans Active Directory.

Tableau 6-1. Privilèges utilisateur iDRAC6

Droits	Description
Ouvrir une session iDRAC	Permet à l'utilisateur d'ouvrir une session iDRAC6.
Configurer iDRAC	Permet à l'utilisateur de configurer iDRAC6.
Configurer les utilisateurs	Permet à l'utilisateur d'autoriser l'accès au système par des utilisateurs spécifiques.
Effacer les journaux	Permet à l'utilisateur d'effacer les journaux iDRAC6.
Exécuter les commandes de contrôle du serveur	Permet à l'utilisateur d'exécuter des commandes RACADM.
Accéder à la redirection de console	Permet à l'utilisateur d'exécuter la redirection de console.
Accéder au média virtuel	Permet à l'utilisateur d'exécuter et d'utiliser le média virtuel.
Tester les alertes	Permet à l'utilisateur d'envoyer des alertes de test (e-mail et PET) à un utilisateur spécifique.
Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Prérequis pour l'activation de l'authentification Active Directory pour iDRAC6

Pour utiliser la fonctionnalité Authentification Active Directory d'iDRAC6, vous devez déjà avoir déployé une infrastructure Active Directory. Consultez le site Web Microsoft pour des informations sur la configuration d'une infrastructure Active Directory si vous n'en avez pas déjà une.

iDRAC6 utilise l'infrastructure à clé publique (PKI) standard pour s'authentifier en toute sécurité sur Active Directory ; vous aurez donc également besoin d'une PKI intégrée dans l'infrastructure Active Directory.

Consultez le site Web Microsoft pour plus d'informations sur la configuration de PKI.

Pour vous authentifier correctement sur tous les contrôleurs de domaine, vous aurez également besoin d'activer le protocole Secure Socket Layer (SSL) sur tous les contrôleurs de domaine auxquels iDRAC6 se connecte. Pour de plus amples informations, voir « Activation de SSL sur un contrôleur de domaine ».

Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès de l'utilisateur à iDRAC6 par l'intermédiaire de deux méthodes : vous pouvez utiliser la solution de *schéma étendu* que Dell a personnalisée pour y ajouter des objets Active Directory définis par Dell. Sinon, vous pouvez utiliser la solution de *schéma standard*, qui utilise uniquement les objets du groupe Active Directory. Pour plus d'informations sur ces solutions, reportez-vous aux sections suivantes.

Lorsque vous utilisez Active Directory pour configurer l'accès à iDRAC6, vous devez choisir la solution de schéma étendu ou standard.

La solution de schéma étendu présente les avantages suivants :

- Tous les objets de contrôle d'accès sont maintenus dans Active Directory.
- La configuration de l'accès des utilisateurs sur différentes cartes iDRAC6 s'illustre par une flexibilité maximale, avec différents niveaux de privilèges.

L'avantage lié à l'utilisation de la solution de schéma standard est qu'aucune extension du schéma n'est nécessaire, car toutes les classes d'objets requises sont fournies via la configuration par défaut du schéma Active Directory dans Microsoft.

Présentation d'Active Directory avec le schéma étendu

L'utilisation de la solution de schéma étendu requiert l'extension du schéma Active Directory, comme décrit dans la section ci-après.

Extension du schéma Active Directory

Important : l'extension de schéma pour ce produit est différente des générations précédentes de la gamme de produits Dell de gestion à distance. Vous devez étendre le nouveau schéma et installer dans votre répertoire le nouveau **snap-in de la console MMC (Microsoft Management Console) : « Utilisateurs et ordinateurs Active Directory »**. L'ancien schéma ne fonctionne pas avec ce produit.

REMARQUE : Le fait d'étendre le nouveau schéma ou d'installer la nouvelle extension pour le snap-in Utilisateurs et ordinateurs Active Directory n'a aucun effet sur les versions antérieures du produit.

L'utilitaire Schema Extender et l'extension du snap-in Utilisateurs et ordinateurs Active Directory pour la console MMC sont disponibles dans le DVD *Dell Systems Management Tools and Documentation*. Pour plus d'informations, reportez-vous aux sections « Extension du schéma Active Directory » et « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory ». Pour plus d'informations sur l'extension du schéma pour iDRAC6 et l'installation du snap-in Utilisateurs et ordinateurs Active Directory pour la console MMC, reportez-vous au *Guide d'installation et de sécurité de Dell OpenManage* disponible sur le site **support.dell.com\manuals**.

REMARQUE : Lorsque vous créez des objets Association iDRAC6 ou des objets Périphérique iDRAC6, veillez à bien sélectionner **l'option avancée de gestion à distance Dell (Dell Remote Management Object Advanced)**.

Extensions de schéma Active Directory

Les données d'Active Directory constituent une base de données distribuée d'attributs et de classes. Le schéma d'Active Directory inclut les règles qui déterminent le type de données qui peuvent être ajoutées ou incluses dans la base de données. La classe d'utilisateur est un exemple de classe qui est conservée dans la base de données. Quelques exemples d'attributs de la classe utilisateur peuvent être le prénom de l'utilisateur, son nom de famille, son numéro de téléphone, etc. Les sociétés peuvent étendre la base de données d'Active Directory en y ajoutant leurs propres attributs et classes uniques pour répondre aux besoins spécifiques à leur environnement. Dell a étendu ce schéma pour inclure les modifications nécessaires à la prise en charge de l'authentification et de l'autorisation de la gestion à distance.

Chaque attribut ou classe ajouté à un schéma d'Active Directory existant peut être défini par un ID unique. Pour que les ID soient uniques dans toute l'industrie, Microsoft tient à jour une base de données d'identificateurs d'objets (OID) Active Directory de sorte que lorsque des sociétés ajoutent des extensions au schéma, elles sont sûres que ces extensions seront uniques et ne créeront pas de conflits avec d'autres. Pour étendre le schéma de Microsoft Active Directory, Dell a reçu des OID uniques, des extensions de noms uniques et des ID d'attributs uniques liés pour les attributs et les classes ajoutés au service de répertoire.

- L'extension de Dell est : `dell`
- L'OID de base de Dell est : `1.2.840.113556.1.8000.1280`
- La plage des ID de liens RAC est : `12070 à 12079`

Présentation des extensions de schéma iDRAC6

Pour offrir la plus grande flexibilité face à la multitude des environnements clients, Dell fournit un groupe de propriétés qui peut être configuré par l'utilisateur en fonction des résultats souhaités. Dell a étendu le schéma pour inclure les propriétés Association, Périphérique et Privilège. La propriété Association est utilisée pour associer les utilisateurs ou les groupes à un ensemble spécifique de privilèges pour un ou plusieurs périphériques iDRAC6. Ce modèle offre à l'administrateur un maximum de flexibilité sur les différentes combinaisons d'utilisateurs, de privilèges iDRAC6 et de périphériques iDRAC6 sur le réseau, sans ajouter trop de complexité.

Aperçu des objets Active Directory

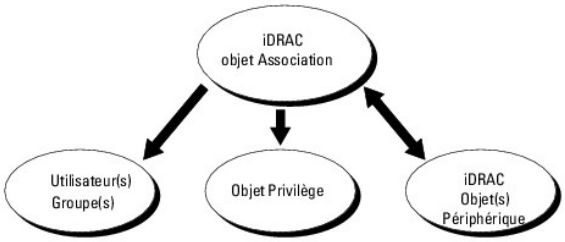
Pour chaque périphérique iDRAC6 physique présent sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, vous devez créer au moins un objet Association et un objet Périphérique iDRAC6. Vous pouvez créer plusieurs objets Association et chaque objet Association peut être lié à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Périphérique iDRAC6 que vous le souhaitez. Les utilisateurs et les objets Périphérique iDRAC6 peuvent être des membres de n'importe quel domaine dans l'entreprise.

Cependant, chaque objet Association ne peut être lié (ou ne peut lier les utilisateurs, les groupes d'utilisateurs ou les objets Périphérique iDRAC6) qu'à un seul objet Privilège. Cet exemple permet à l'administrateur de contrôler les privilèges de chaque utilisateur sur des périphériques iDRAC6 spécifiques.

L'objet Périphérique iDRAC6 est le lien vers le micrologiciel d'iDRAC6 permettant à Active Directory d'effectuer une requête d'authentification et d'autorisation. Quand iDRAC6 est ajouté au réseau, l'administrateur doit configurer l'iDRAC6 et son objet de périphérique avec son nom Active Directory pour que les utilisateurs puissent établir l'authentification et l'autorisation avec Active Directory. En outre, l'administrateur doit ajouter iDRAC6 à au moins un objet Association pour que les utilisateurs puissent s'authentifier.

Figure 6-1 illustre le fait que l'objet Association fournit la connexion nécessaire pour toute authentification et autorisation.

Figure 6-1. Configuration typique pour les objets Active Directory



Vous pouvez créer autant d'objets Association que vous le voulez. Cependant, vous devez créer au moins un objet Association et vous devez avoir un objet Périphérique iDRAC6 pour chaque périphérique iDRAC6 du réseau que vous voulez intégrer à Active Directory pour en gérer l'authentification et l'autorisation.

L'objet Association inclut autant d'utilisateurs et/ou de groupes que d'objets Périphérique iDRAC6. Toutefois, l'objet Association ne peut inclure qu'un objet Privilège par objet Association. L'objet Association connecte les *utilisateurs* qui ont des *privilèges* sur les périphériques iDRAC6.

L'extension Dell du snap-in MMC ADUC permet uniquement d'associer l'objet Privilège et les objets iDRAC6 d'un même domaine à l'objet Association. Elle ne permet pas d'ajouter un groupe ou un objet iDRAC6 provenant d'un autre domaine en tant que membre produit de l'objet Association.

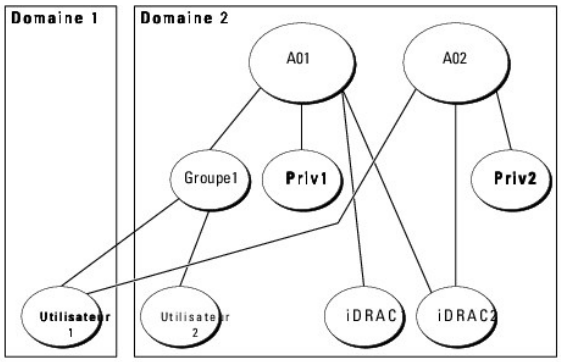
Les utilisateurs, les groupes d'utilisateurs et les groupes d'utilisateurs imbriqués de n'importe quel domaine peuvent être ajoutés à l'objet Association. Les solutions de schéma étendu prennent en charge tous les types de groupes d'utilisateurs et l'imbrication de groupes d'utilisateurs dans plusieurs domaines autorisés par Microsoft Active Directory.

Accumulation de privilèges à l'aide du schéma étendu

Le mécanisme d'authentification du schéma étendu prend en charge l'accumulation de privilèges depuis différents objets Privilège associés au même utilisateur via différents objets Association. En d'autres termes, l'authentification du schéma étendu accumule les privilèges pour accorder à l'utilisateur le super ensemble de tous les privilèges attribués correspondant aux différents objets Privilège associés au même utilisateur.

Figure 6-2 fournit un exemple d'accumulation de privilèges à l'aide du schéma étendu.

Figure 6-2. Accumulation de privilèges pour un utilisateur



La figure illustre deux objets Association, A01 et A02. Utilisateur1 est associé à iDRAC2 via les deux objets Association. Par conséquent, Utilisateur1 a accumulé des privilèges résultant de l'association de l'ensemble des privilèges pour les objets Priv1 et Priv2 sur iDRAC2.

Par exemple, Priv1 possède les privilèges Ouvrir une session, Média virtuel et Effacer les journaux et Priv2 a les privilèges Ouvrir une session, Configurer iDRAC et Tester les alertes. Par conséquent, Utilisateur1 aura maintenant l'ensemble de privilèges Ouvrir une session, Média virtuel, Effacer les journaux, Configurer iDRAC et Tester les alertes, qui correspond à l'ensemble de privilèges associé de Priv1 et Priv2.

L'authentification du schéma étendu accumule les privilèges pour accorder à l'utilisateur l'ensemble maximum de privilèges possibles, en tenant compte des privilèges attribués des différents objets Privilège associés au même utilisateur.

Dans cette configuration, Utilisateur1 possède à la fois les privilèges de Priv1 et Priv2 sur iDRAC2. Utilisateur1 a les privilèges de Priv1 sur iDRAC1 seulement. Utilisateur2 a les privilèges de Priv1 à la fois sur iDRAC1 et sur iDRAC2. Par ailleurs, cette illustration indique qu'Utilisateur1 peut appartenir à un autre domaine et peut être membre d'un groupe.

Configuration du schéma étendu d'Active Directory pour accéder à iDRAC6

Pour pouvoir utiliser Active Directory pour accéder à iDRAC6, configurez le logiciel Active Directory et iDRAC6 en effectuant les étapes suivantes dans l'ordre :

1. Étendez le schéma Active Directory (voir « Extension du schéma Active Directory »).
2. Étendez le snap-in Utilisateurs et ordinateurs Active Directory (voir « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory »).
3. Ajoutez des utilisateurs iDRAC6 et leurs privilèges à Active Directory (voir « Ajout d'utilisateurs iDRAC6 et de leurs privilèges à Active Directory »).

4. Activez SSL sur chacun de vos contrôleurs de domaine (voir « Activation de SSL sur un contrôleur de domaine »).

5. Configurez les propriétés Active Directory d'iDRAC6 via l'interface Web d'iDRAC6 ou RACADM (voir « Configuration d'Active Directory avec le schéma étendu via l'interface Web d'iDRAC6 » ou « Configuration d'Active Directory avec le schéma étendu via RACADM »).

En étendant le schéma Active Directory, vous ajoutez une unité d'organisation Dell, des classes et des attributs de schéma, et des exemples d'objets de Privilège et Association au schéma Active Directory. Pour étendre le schéma, vous devez avoir des privilèges Administrateur de schéma pour le propriétaire de rôle FSMO (Flexible Single Master Operation) contrôleur de schéma de la forêt de domaine.

Vous pouvez étendre votre schéma en utilisant une des méthodes suivantes :

- l'utilitaire Dell Schema Extender ;
- le fichier script LDIF.

Si vous utilisez le fichier script LDIF, l'unité organisationnelle Dell ne sera pas ajoutée au schéma.

Les fichiers LDIF et Dell Schema Extender sont situés sur votre DVD *Dell Systems Management Tools and Documentation* dans les répertoires respectifs suivants :

- *Lecteur de DVD* **:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- *<lecteur de* ***DVD****>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender*

Pour utiliser les fichiers LDIF, reportez-vous aux instructions du fichier lisez-moi qui se trouve dans le répertoire **LDIF_Files**. Pour utiliser l'utilitaire Dell Schema Extender pour étendre le schéma Active Directory, voir « Utilisation de Dell Schema Extender ».

Vous pouvez copier et exécuter Schema Extender ou les fichiers LDIF depuis n'importe quel emplacement.

Utilisation de Dell Schema Extender

PRÉCAUTION : L'utilitaire Dell Schema Extender utilise le fichier SchemaExtenderOem.ini. Pour que l'utilitaire Dell Schema Extender fonctionne correctement, ne modifiez pas le nom de ce fichier.

1. Dans l'écran **Bienvenue**, cliquez sur **Suivant**.
2. Lisez et saisissez l'avertissement, puis cliquez sur **Suivant**.
3. Sélectionnez **Utiliser les références d'ouverture de session actuelles** ou saisissez un nom d'utilisateur et un mot de passe ayant des droits d'administrateur de schéma.
4. Cliquez sur **Suivant** pour exécuter Dell Schema Extender.
5. Cliquez sur **Terminer**.

   Le schéma est étendu. Pour vérifier l'extension de schéma, utilisez la console MMC et le snap-in du schéma Active Directory pour vérifier les éléments suivants :

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

   Consultez votre documentation Microsoft pour plus de détails sur l'utilisation de la console MMC et du snap-in du schéma Active Directory.

Tableau 6-2. Définitions de classe pour les classes ajoutées au schéma Active Directory

Nom de classe	Numéro d'identification d'objet attribué (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tableau 6-3. Classe dellRacDevice

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
Description	Représente le périphérique iDRAC6 de Dell. iDRAC6 doit être configuré comme delliDRACDevice dans Active Directory. Cette configuration permet à iDRAC6 d'envoyer des requêtes de protocole LDAP (Lightweight Directory Access Protocol) à Active Directory.
Type de classe	Classe structurelle

SuperClasses	dellProduct
Attributs	**dellSchemaVersion** **dellRacType**

Tableau 6-4. Classe delliDRACAssociationObject

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
Description	Représente l'objet Association de Dell. L'objet Association fournit la connexion entre les utilisateurs et les périphériques.
Type de classe	Classe structurelle
SuperClasses	Groupe
Attributs	**dellProductMembers** **dellPrivilegeMember**

Tableau 6-5. Classe dellRAC4Privileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Description	Définit les privilèges (droits d'autorisation) du périphérique iDRAC6.
Type de classe	Classe auxiliaire
SuperClasses	None (Aucun)
Attributs	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tableau 6-6. Classe dellPrivileges

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

Tableau 6-7. Classe dellProduct

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

Tableau 6-8. Liste des attributs ajoutés au schéma Active Directory

Nom / description de l'attribut	OID attribué/Identificateur d'objet de syntaxe	Valeur unique
dellPrivilegeMember Liste des objets dellPrivilege qui appartiennent à cet Attribut.	1.2.840.113556.1.8000.1280.1.1.2.1 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

dellProductMembers Liste des objets dellRacDevice et DelliDRACDevice qui appartiennent à ce rôle. Cet attribut est le lien vers l'avant vers le lien vers l'arrière dellAssociationMembers. Numéro de lien : 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si l'utilisateur a des droits Ouvrir une session sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.3 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si l'utilisateur a des droits Configuration de carte sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.4 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si l'utilisateur a des droits Configuration d'utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE si l'utilisateur a des droits Effacement de journal sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.6 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si l'utilisateur a des droits Réinitialisation de serveur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.7 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si l'utilisateur a des droits Redirection de console sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.8 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si l'utilisateur a des droits Média virtuel sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.9 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si l'utilisateur a des droits Tests d'alerte utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si l'utilisateur a des droits Administrateur pour la commande de débogage sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.11 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La version de schéma courante est utilisée pour mettre à jour le schéma.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Cet attribut est le type courant de RAC pour l'objet delliDRACDevice et le lien vers l'arrière vers le lien vers l'avant dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut dellProductMembers. ID de lien : 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs Active Directory pour que l'administrateur puisse gérer les périphériques iDRAC6, les utilisateurs et les groupes d'utilisateurs, les associations iDRAC6 et les privilèges iDRAC6.

Lorsque vous installez votre logiciel Systems Management à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez étendre le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** pendant la procédure d'installation. Consultez le *Guide d'installation rapide du logiciel Dell OpenManage* pour des instructions supplémentaires sur l'installation du logiciel Systems Management. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du snap-in se trouve sous :

<lecteur de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs d'Active Directory, consultez votre documentation Microsoft.

Installation du pack administrateur

Vous devez installer le pack administrateur sur tous les systèmes qui gèrent les objets iDRAC6 d'Active Directory. Si vous n'installez pas le pack administrateur, vous ne pouvez pas visualiser l'objet iDRAC6 Dell dans le conteneur.

Pour plus d'informations, voir «Ouverture du snap-in Utilisateurs et ordinateurs Active Directory».

Ouverture du snap-in Utilisateurs et ordinateurs Active Directory

Pour ouvrir le snap-in Utilisateurs et ordinateurs Active Directory :

1. Si vous êtes connecté au contrôleur de domaine, cliquez sur **Démarrer Outils d'administration**→ **Utilisateurs et ordinateurs Active Directory**.

   Si vous n'avez pas ouvert une session sur le contrôleur de domaine, la version appropriée du pack administrateur Microsoft doit être installée sur votre système local. Pour installer ce pack administrateur, cliquez sur **Démarrer**→ **Exécuter**, tapez `MMC` et appuyez sur **Entrée**.

   La console MMC s'affiche.

2. Dans la fenêtre **Console 1**, cliquez sur **Fichier** (ou sur **Console** sur les systèmes exécutant Windows 2000).

3. Cliquez sur **Ajouter/Supprimer un snap-in**.

4. Sélectionnez le **snap-in Utilisateurs et ordinateurs Active Directory**, puis cliquez sur **Ajouter**.

5. Cliquez sur **Fermer** et cliquez sur **OK**.

Ajout d'utilisateurs iDRAC6 et de leurs privilèges à Active Directory

Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous permet d'ajouter des utilisateurs iDRAC6 et des privilèges en créant des objets iDRAC6, Association et Privilège. Pour ajouter chaque type d'objet, effectuez les procédures suivantes :

- Créez un objet Périphérique iDRAC6
- Créez un objet Privilège
- Créez un objet Association
- Ajoutez des objets à un objet Association

Création d'un objet Périphérique iDRAC6

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

2. Sélectionnez **Nouveau**→ **Dell Remote Management Object Advanced (option avancée de gestion à distance Dell)**.

   La fenêtre **Nouvel objet** apparaît.

3. Entrez un nom pour le nouvel objet. Ce nom doit être identique au nom iDRAC6 saisi à l'étape A de la section « Configuration d'Active Directory avec le schéma étendu via l'interface Web d'iDRAC6 ».

4. Sélectionnez **l'objet Périphérique iDRAC**.

5. Cliquez sur **OK**.

Création d'un objet Privilège

REMARQUE : Un objet Privilège doit être créé dans le même domaine que l'objet Association associé.

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

2. Sélectionnez **Nouveau**→ **Dell Remote Management Object Advanced (option avancée de gestion à distance Dell)**.

   La fenêtre **Nouvel objet** apparaît.

3. Entrez un nom pour le nouvel objet.

4. Sélectionnez **Objet Privilège**.

5. Cliquez sur **OK**.

6. Cliquez-droite sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.

7. Cliquez sur l'onglet **Remote Management Privileges (Privilèges de gestion à distance)** et sélectionnez les privilèges que vous souhaitez attribuer à l'utilisateur ou au groupe (voir Tableau 5-10).

Création d'un objet Association

REMARQUE : L'objet Association iDRAC6 est dérivé du groupe, et sa portée est définie sur le domaine local.

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

2. Sélectionnez **Nouveau→ Dell Remote Management Object Advanced (option avancée de gestion à distance Dell)**.

   Cela ouvre la fenêtre **Nouvel objet**.

3. Entrez un nom pour le nouvel objet.

4. Sélectionnez **Objet Association**.

5. Sélectionnez l'étendue de **l'objet Association**.

6. Cliquez sur **OK**.

Ajout d'objets à un objet Association

Dans la fenêtre **Propriétés de l'objet Association**, vous pouvez associer des utilisateurs, des groupes d'utilisateurs, des objets Privilège et des périphériques iDRAC6 ou des groupes de périphériques iDRAC6.

Vous pouvez ajouter des groupes d'utilisateurs et de périphériques iDRAC6. 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. Entrez le nom de l'utilisateur ou du groupe d'utilisateurs et cliquez sur **OK**.

Ajout de privilèges

1. Sélectionnez l'onglet **Objet Privilèges** et cliquez sur **Ajouter**.

2. Entrez le nom de l'objet Privilège et cliquez sur **OK**.

Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs durant l'authentification auprès d'un périphérique iDRAC6. Vous ne pouvez ajouter qu'un seul objet Privilège à un objet Association.

Ajout de périphériques iDRAC6 ou de groupes de périphériques iDRAC6

Pour ajouter des périphériques iDRAC6 ou des groupes de périphériques iDRAC6 :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter.**

2. Saisissez le nom des périphériques iDRAC6 ou du groupe de périphériques iDRAC6, puis cliquez sur **OK**.

3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

Cliquez sur l'onglet **Produits** pour ajouter un périphérique iDRAC6 connecté au réseau et disponible pour les utilisateurs ou groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques iDRAC6 à un objet Association.

Configuration d'Active Directory avec le schéma étendu via l'interface Web d'iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Connectez-vous à l'interface Web d'iDRAC6.
3. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ **iDRAC**.

   L'écran **Informations iDRAC** s'affiche.
4. Cliquez sur l'onglet **Sécurité réseau**, puis sur **Active Directory**.

   La page **Configuration et gestion d'Active Directory** apparaît.
5. Faites dérouler l'écran vers le bas, puis cliquez sur **Configurer Active Directory**.

   L'écran **Étape 1/4 Configuration et gestion d'Active Directory** s'affiche.
6. Pour valider le certificat SSL de vos serveurs Active Directory, cochez la case **Enable Certificate Validation (Activer la validation de certificat)** dans le menu des paramètres de certificat (**Certificate Settings**).

   Si vous ne souhaitez pas valider le certificat SSL de vos serveurs Active Directory, n'effectuez aucune opération, et passez à l'étape étape 8.
7. Sous **Télécharger le certificat CA d'Active Directory**, indiquez le chemin d'accès au fichier du certificat ou parcourez le serveur pour accéder à ce fichier, puis cliquez sur **Télécharger**.

   REMARQUE : Vous devez indiquer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets, ainsi que l'extension du fichier.

   Les informations relatives au certificat CA d'Active Directory que vous avez téléchargé figurent dans la section relative au certificat CA courant (**Current Active Directory CA Certificate**).
8. Cliquez sur **Suivant**.

   L'écran **Étape 2/4 Configuration et gestion d'Active Directory** s'affiche.
9. Cochez la case **Activer Active Directory**.
10. Cliquez sur **Ajouter** pour indiquer le nom du domaine utilisateur, entrez ce nom dans la zone de texte, puis cliquez sur **OK**.
11. En réponse à l'invite, saisissez le nom du domaine utilisateur, puis cliquez sur **OK**. Remarque : cette étape est facultative. Si vous configurez une liste de domaines utilisateur, celle-ci sera disponible dans l'écran de connexion à l'interface Web. Vous pouvez sélectionner un domaine dans la liste. Ainsi, vous devrez simplement indiquer le nom de l'utilisateur.
12. Dans le champ **Délai d'attente**, indiquez le délai d'attente (en secondes) pour que les requêtes d'iDRAC6 soient traitées par Active Directory. La valeur par défaut est 120 secondes.
13. Indiquez l'**adresse serveur du contrôleur de domaine**. Vous pouvez définir jusqu'à 3 serveurs Active Directory pour le traitement des connexions, mais vous devez configurer au moins un serveur. Pour ce faire, indiquez son adresse IP ou le nom de domaine entièrement qualifié (FQDN). iDRAC6 tente de se connecter à chacun des serveurs configurés jusqu'à se qu'une connexion soit établie.

REMARQUE : Si la validation de certificat est activée, le FQDN ou l'adresse IP que vous définissez dans ce champ doivent correspondre au champ **Demandeur** ou **Subject Alternative Name (autre nom du demandeur)** de votre certificat de contrôleur de domaine.

14. Cliquez sur **Suivant**.

    L'écran **Étape 3/4 Configuration et gestion d'Active Directory** s'affiche.
15. Sous **Sélection du schéma**, cochez la case **Schéma étendu**.
16. Cliquez sur **Suivant**.

    L'écran **Étape 4/4 Configuration et gestion d'Active Directory** s'affiche.
17. Sous **Paramètres du schéma étendu**, entrez le nom iDRAC6 et le nom de domaine iDRAC6 pour configurer l'objet de périphérique iDRAC6 et son emplacement dans Active Directory.
18. Cliquez sur **Terminer** pour enregistrer vos modifications, puis sur **Terminé**.

    La page principale **Configuration et gestion d'Active Directory** apparaît. Ensuite, vous devez tester les paramètres d'Active Directory que vous venez de configurer.

19. Faites défiler l'écran vers le bas, puis cliquer sur **Test Settings (Tester les paramètres)**.

    L'écran **Test Active Directory Settings** (Tester les paramètres d'Active Directory) s'affiche.

20. Saisissez votre nom d'utilisateur iDRAC6 et votre mot de passe, puis cliquez sur **Start Test (Lancer le test)**.

    Les résultats et le journal de test s'affichent. Pour plus d'informations, voir « Test de vos configurations ».

REMARQUE : Vous devez posséder un serveur de DNS correctement configuré sur iDRAC6 pour prendre en charge la connexion à Active Directory. Pour configurer le(s) serveur(s) DNS manuellement ou utiliser le protocole DHCP pour obtenir des serveurs DNS, accédez à l'écran **Configuration du réseau** (cliquez sur **Système**→ **Accès à distance**→ **iDRAC**, puis sélectionnez l'onglet **Réseau/Sécurité**).

La configuration d'Active Directory avec la solution de schéma étendu est maintenant terminée.

Configuration d'Active Directory avec le schéma étendu via RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory d'iDRAC6 avec le schéma étendu en utilisant l'outil CLI (interface de ligne de commande) RACADM au lieu de l'interface Web.

1. Ouvrez une invite de commande et tapez les commandes RACADM suivantes :

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1

   racadm config -g cfgActiveDirectory -o cfgADType 1

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

   racadm config -g cfgActiveDirectory -o cfgADRacDomain <nom de domaine rac pleinement qualifié>

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>
   ```

   REMARQUE : Vous devez configurer au moins une de ces trois adresses. iDRAC6 tente de se connecter successivement à chacune des adresses configurées, jusqu'à ce qu'une connexion soit établie. Dans le cas du schéma étendu, ce sont les adresses IP ou le FQDN des contrôleurs de domaine dans lesquels se trouve le périphérique iDRAC6. Les serveurs de catalogue global ne sont pas du tout utilisés dans le mode de schéma étendu.

   Si vous souhaitez désactiver la validation de certificat lors de l'établissement d'une liaison SSL, exécutez la commande RACADM suivante :

   ```
   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
   ```

   Dans ce cas, il n'est pas nécessaire de télécharger un certificat CA.

   Si vous souhaitez activer la validation de certificat lors de l'établissement d'une liaison SSL, exécutez la commande RACADM suivante :

   ```
   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
   ```

   Dans ce cas, vous devez télécharger un certificat CA à l'aide de la commande RACADM suivante :

   ```
   racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>
   ```

   L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, voir « Importation du certificat SSL du micrologiciel iDRAC6 ».

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

2. Si DHCP est activé sur iDRAC6 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 iDRAC6 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 de DNS principale>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP de DNS secondaire>
   ```

4. Si vous souhaitez configurer une liste des domaines utilisateur afin de n'avoir à saisir le nom utilisateur que lors de la connexion à l'interface Web d'iDRAC6, tapez la commande suivante :

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName -i <index>
   ```

Vous pouvez configurer jusqu'à 40 domaines utilisateur avec des numéros d'index compris entre 1 et 40.

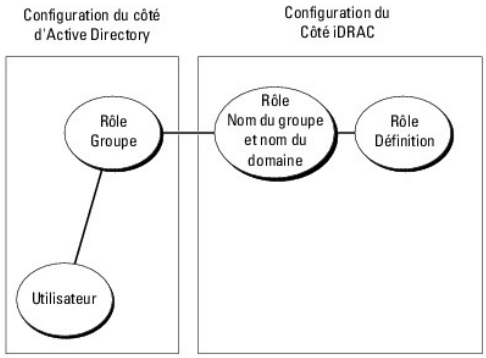
Pour plus d'informations sur les domaines utilisateur, consultez la section « Utilisation d'Active Directory pour ouvrir une session iDRAC6 ».

5. Appuyez sur la touche **Entrée** pour terminer la configuration d'Active Directory avec le schéma étendu.

Présentation d'Active Directory avec le schéma standard

Comme illustré dans la Figure 6-3, l'utilisation du schéma standard pour l'intégration d'Active Directory nécessite une configuration sur Active Directory et sur iDRAC6.

Figure 6-3. Configuration d'iDRAC6 avec Microsoft Active Directory et le schéma standard



Du côté d'Active Directory, un objet de groupe standard est utilisé comme groupe de rôles. Un utilisateur ayant accès à iDRAC6 sera membre du groupe de rôles. Pour octroyer à cet utilisateur l'accès à une carte iDRAC6 spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cette carte iDRAC6. Contrairement à la solution du schéma étendu, le niveau des rôles et des privilèges est défini sur chaque carte iDRAC6 et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque iDRAC6.La Tableau 6-9 affiche les privilèges des groupes de rôles par défaut.

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

Groupes de rôles	Niveau de privilège par défaut	Droits accordés	Masque binaire
Groupe de rôles 1	Administrateur	**Ouvrir une session iDRAC**, **Configurer iDRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**, **Exécuter des commandes de diagnostic**	0x000001ff
Groupe de rôles 2	Opérateur	**Ouvrir une session iDRAC**, **Configurer iDRAC, Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes, Exécuter des commandes de diagnostic**	0x000000f9
Groupe de rôles 3	Lecture seule	Ouvrir une session iDRAC	0x00000001
Groupe de rôles 4	None (Aucun)	Aucun droit attribué	0x00000000
Groupe de rôles 5	None (Aucun)	Aucun droit attribué	0x00000000

REMARQUE : Les valeurs Masque binaire sont utilisées uniquement lors de la définition du schéma standard avec la RACADM.

Scénarios de domaines uniques et de domaines multiples

Si tous les utilisateurs et les groupes de rôles, y compris les groupes imbriqués, se trouvent dans le même domaine, alors seules les adresses des contrôleurs de domaine doivent être configurées sur iDRAC6. Dans ce scénario de domaine unique, tous les types de groupes sont pris en charge.

Si tous les utilisateurs et les groupes de rôles, y compris les groupes imbriqués, proviennent de différents domaines, alors les adresses de serveur de catalogue global doivent être configurées sur iDRAC6. Dans ce scénario de domaines multiples, tous les groupes de rôles et groupes imbriqués éventuels doivent être de type universel.

Configuration du schéma standard d'Active Directory pour accéder à iDRAC6

Vous devez effectuer les étapes suivantes pour configurer Active Directory avant qu'un utilisateur Active Directory puisse avoir accès à iDRAC6 :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le **snap- in Utilisateurs et ordinateurs Active Directory.**

2. Créez un groupe ou sélectionnez un groupe existant. Le nom du groupe et le nom de ce domaine doivent être configurés sur iDRAC6 via l'interface Web ou via RACADM (voir « Configuration d'Active Directory avec le schéma standard via l'interface Web d'iDRAC6 » ou « Configuration d'Active Directory avec le schéma standard via RACADM »).

3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse accéder à iDRAC6.

Configuration d'Active Directory avec le schéma standard via l'interface Web d'iDRAC6

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

2. Connectez-vous à l'interface Web iDRAC6.

3. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ **iDRAC**.

4. Cliquez sur l'onglet **Sécurité réseau**, puis sur **Active Directory**.

   La page **Configuration et gestion d'Active Directory** apparaît.

5. Faites dérouler l'écran vers le bas, puis cliquez sur **Configurer Active Directory**.

   L'écran **Étape 1/4 Configuration et gestion d'Active Directory** s'affiche.

6. Dans le menu des paramètres de certificat (**Certificate Settings**), sélectionnez **Activer Active Directory**.

7. Sous **Télécharger le certificat CA d'Active Directory**, indiquez le chemin d'accès au fichier du certificat ou parcourez le serveur pour accéder à ce fichier, puis cliquez sur **Télécharger**.

   REMARQUE : Vous devez indiquer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets, ainsi que l'extension du fichier.

   Les informations relatives au certificat CA d'Active Directory que vous avez téléchargé figurent dans la section relative au certificat CA courant (**Current Active Directory CA Certificate**).

8. Cliquez sur Suivant.

   L'écran **Étape 2/4 Configuration et gestion d'Active Directory** s'affiche.

9. Cochez la case **Activer Active Directory**.

10. Cliquez sur **Ajouter** pour indiquer le nom du domaine utilisateur, entrez ce nom dans la zone de texte, puis cliquez sur **OK**.

11. Dans le champ **Délai d'attente**, indiquez le délai d'attente (en secondes) pour que les requêtes d'iDRAC6 soient traitées par Active Directory. La valeur par défaut est 120 secondes.

12. Indiquez l'**adresse serveur du contrôleur de domaine**. Vous pouvez définir jusqu'à 3 serveurs Active Directory pour le traitement des connexions, mais vous devez configurer au moins un serveur. Pour ce faire, indiquez son adresse IP ou le nom de domaine entièrement qualifié (FQDN). iDRAC6 tente de se connecter à chacun des serveurs configurés jusqu'à se qu'une connexion soit établie.

13. Cliquez sur **Suivant**.

    L'écran **Étape 3/4 Configuration et gestion d'Active Directory** s'affiche.

14. Sous **Sélection du schéma**, cochez la case **Schéma standard**.

15. Cliquez sur **Suivant**.

    L'écran **Étape 4a/4 Configuration et gestion d'Active Directory** s'affiche.

16. Dans la section **Paramètres du schéma standard**, entrez les adresses de serveur de catalogue global.

REMARQUE : Le serveur de catalogue global est requis uniquement pour le schéma standard, lorsque les comptes utilisateur et les groupes de rôles proviennent de domaines différents. Dans ce scénario de domaines multiples, seul le groupe universel peut être utilisé.

17. Cliquez sur un bouton **Groupe de rôles** pour ajouter un groupe de rôles.

    L'écran **Étape 4b/4 Configurer le groupe de rôles 1** s'affiche.

18. Saisissez le **Nom du groupe**. Le nom du groupe identifie le groupe de rôles d'Active Directory associé à iDRAC6.

19. Indiquez le **Domaine du groupe**. Le **Domaine du groupe** est le nom de domaine racine pleinement qualifié de la forêt.

20. Dans la section **Privilèges du groupe de rôles**, définissez les privilèges du groupe. Pour plus d'informations sur les privilèges des groupes de rôles, reportez-vous à la Tableau 5-11 sous .

    REMARQUE : 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.

21. Cliquez sur **OK** pour enregistrer les paramètres des groupes de rôles.

    Une boîte de dialogue d'alerte s'affiche et indique que vos paramètres ont été modifiés. Cliquez sur OK pour revenir à l'écran **Étape 4a/4 Configuration et gestion d'Active Directory**.

22. Pour ajouter un autre groupe de rôles, répétez les étapes étape 17 à étape 21.

23. Cliquez sur **Terminer**, puis sur **Terminé**.

    La page principale **Configuration et gestion d'Active Directory** apparaît. Ensuite, vous devez tester les paramètres d'Active Directory que vous venez de configurer.

24. Faites défiler l'écran vers le bas, puis cliquer sur **Test Settings (Tester les paramètres)**.

    L'écran **Test Active Directory Settings** (Tester les paramètres d'Active Directory) s'affiche.

25. Saisissez votre nom d'utilisateur iDRAC6 et votre mot de passe, puis cliquez sur **Start Test (Lancer le test)**.

    Les résultats et le journal de test s'affichent. Pour plus d'informations, reportez-vous à la section « Test de vos configurations ».

REMARQUE : Vous devez posséder un serveur de DNS correctement configuré sur iDRAC6 pour prendre en charge la connexion à Active Directory. Accédez à la page **Accès à distance**→ **Configuration**→ **Réseau** pour configurer les serveurs DNS manuellement ou pour les obtenir via le protocole DHCP.

La configuration d'Active Directory avec la solution de schéma standard est maintenant terminée.

Configuration d'Active Directory avec le schéma standard via RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory d'iDRAC6 avec le schéma standard en utilisant l'interface CLI RACADM au lieu de l'interface Web.

1. Ouvrez une invite de commande et tapez les commandes RACADM suivantes :

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1

   racadm config -g cfgActiveDirectory -o cfgADType 2

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

   racadm config -g cfgStandardSchema -i <index> -o
   cfgSSADRoleGroupDomain <nom de domaine entièrement qualifié>

   racadm config -g cfgStandardSchema -i <index> -o
   cfgSSADRoleGroupPrivilege <numéro du masque binaire pour des droits d'utilisateur spécifiques>
   ```

   REMARQUE : Pour les valeurs numériques Masque binaire, voir Tableau B-1.

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>
   ```

   REMARQUE : Indiquez le FQDN du contrôleur de domaine, *pas* le FQDN du domaine. Par exemple, saisissez `servername.dell.com` au lieu de `dell.com`.

   REMARQUE : Au moins une des 3 adresses doit être configurées. iDRAC6 tente de se connecter successivement à chacune des adresses configurées, jusqu'à ce qu'une connexion soit établie. Dans le cas du schéma standard, ce sont les adresses des contrôleurs de domaine dans lesquels se trouvent les comptes utilisateur et les groupes de rôles.

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <nom de domaine entièrement qualifié ou adresse IP du contrôleur de domaine>
   ```

   REMARQUE : Le serveur de catalogue global est requis uniquement pour le schéma standard, lorsque les comptes utilisateur et les groupes de rôles proviennent de domaines différents. Dans ce scénario de domaines multiples, seul le groupe universel peut être utilisé.

REMARQUE : Si la validation de certificat est activée, le FQDN ou l'adresse IP que vous définissez dans ce champ doivent correspondre au champ **Demandeur** ou **Subject Alternative Name (autre nom du demandeur)** de votre certificat de contrôleur de domaine.

Si vous souhaitez désactiver la validation de certificat lors de l'établissement d'une liaison SSL, exécutez la commande RACADM suivante :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

Dans ce cas, il n'est pas nécessaire de télécharger un certificat émis par une autorité de certification (CA).

Si vous souhaitez activer la validation de certificat lors de l'établissement d'une liaison SSL, exécutez la commande RACADM suivante :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

Dans ce cas, vous devez également télécharger le certificat CA à l'aide de la commande RACADM suivante :

```
racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>
```

L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, voir « Importation du certificat SSL du micrologiciel iDRAC6 ».

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

2. Si DHCP est activé sur iDRAC6 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 iDRAC6 ou que vous voulez entrer manuellement les adresses IP du DNS, tapez les commandes RACADM suivantes :

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP de DNS principale>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP du DNS secondaire>
```

4. Si vous souhaitez configurer une liste des domaines utilisateur afin de n'avoir à saisir le nom utilisateur que lors de la connexion à l'interface Web, tapez la commande suivante :

```
racadm config -g cfgUserDomain -o cfgUserDomainName -i <index>
```

Vous pouvez configurer jusqu'à 40 domaines utilisateur avec des numéros d'index compris entre 1 et 40.

Pour plus d'informations sur les domaines utilisateur, consultez la section « Utilisation d'Active Directory pour ouvrir une session iDRAC6 ».

Test de vos configurations

Si vous souhaitez vérifier que votre configuration fonctionne ou si vous souhaitez diagnostiquer le problème à l'origine de l'échec de l'ouverture de session Active Directory, vous pouvez tester vos paramètres dans l'interface Web d'iDRAC6.

Lorsque vous avez terminé de définir vos paramètres dans l'interface Web d'iDRAC6, cliquez sur **Test Settings** (Tester les paramètres) en bas de l'écran. Vous serez invité à indiquer le nom d'un utilisateur test (par exemple, nom utilisateur@domaine.com) et un mot de passe pour exécuter le test. En fonction de votre configuration, la procédure de test peut être plus ou moins longue et il se peut que les résultats s'affichent pour chaque étape. Un journal de test détaillé s'affiche en bas de l'écran des résultats.

Si une étape rencontre un échec, consultez les détails du journal de test pour identifier le problème et trouver une solution. Pour consulter les erreurs les plus fréquentes, reportez-vous à la section « Questions les plus fréquentes ».

Si vous avez besoin d'apporter des modifications à vos paramètres, cliquez sur l'onglet **Active Directory** et modifiez la configuration étape par étape.

Activation de SSL sur un contrôleur de domaine

Quand iDRAC6 authentifie les utilisateurs par rapport à un contrôleur de domaine d'Active Directory, il démarre une session SSL avec le contrôleur de domaine. À ce moment, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (CA), dont le certificat racine est également téléchargé sur iDRAC6. En d'autres termes, pour que l'iDRAC6 puisse s'authentifier sur *n'importe quel* contrôleur de domaine, qu'il s'agisse du contrôleur de domaine racine ou enfant, ce contrôleur de domaine doit avoir un certificat activé SSL signé par la CA du domaine.

Si vous utilisez la CA racine d'entreprise Microsoft pour attribuer *automatiquement* un certificat SSL à tous vos contrôleurs de domaine, effectuez les étapes suivantes pour activer SSL sur chaque contrôleur de domaine.

1. Activez SSL sur chacun de vos contrôleurs de domaine en installant le certificat SSL pour chaque contrôleur.
   a. Cliquez sur **Démarrer**→ **Outils d'administration**→ **Règle de sécurité du domaine**.
   b. Développez le dossier **Règles de clé publique**, cliquez-droite sur **Paramètres de demande automatique de certificat** et cliquez sur **Demande automatique de certificat**.
   c. Dans l'**Assistant Configuration de demandes automatiques de certificats**, cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.
   d. Cliquez sur **Suivant** et cliquez sur **Terminer**.

Exportation du certificat d'autorité de certification racine du contrôleur de domaine vers iDRAC6

REMARQUE : Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

REMARQUE : Si vous utilisez une autorité de certification indépendante, les étapes ci-après peuvent être différentes.

1. Localisez le contrôleur de domaine qui exécute le service CA d'entreprise Microsoft.
2. Cliquez sur **Démarrer** → **Exécuter**.
3. Dans le champ **Exécuter**, tapez `mmc`, puis cliquez sur **OK**.
4. Dans la fenêtre **Console 1** (MMC), cliquez sur **Fichier (**ou **Console** pour les systèmes **Windows 2000),** puis sélectionnez **Ajouter/Supprimer un snap-in**.
5. Dans la fenêtre **Ajouter/Supprimer un snap-in**, cliquez sur **Ajouter**.
6. Dans la fenêtre **Snap-in autonome,** sélectionnez **Certificats** et cliquez sur **Ajouter**.
7. Sélectionnez le compte **Ordinateur** et cliquez sur **Suivant**.
8. Sélectionnez **Ordinateur local** et cliquez sur **Terminer**.
9. Cliquez sur **OK**.
10. Dans la fenêtre **Console 1**, développez le dossier **Certificats**, puis le dossier **Personnel** et cliquez sur le dossier **Certificats**.
11. Repérez le certificat d'autorité de certification racine, cliquez dessus avec le bouton droit de la souris et sélectionnez **Toutes les tâches**, puis cliquez sur **Exporter...**.
12. Dans l'**Assistant Exportation de certificat**, cliquez sur **Suivant** et sélectionnez **Ne pas exporter la clé privée**.
13. Cliquez sur **Suivant** et sélectionnez **Codé à base 64 X.509 (.cer)** comme format.
14. Cliquez sur **Suivant** et enregistrez le certificat dans un répertoire de votre système.
15. Téléchargez le certificat que vous avez enregistré dans étape 14 sur iDRAC6.

    Pour télécharger le certificat à l'aide des commandes RACADM, voir « Configuration d'Active Directory avec le schéma standard via RACADM ».

    Pour télécharger le certificat à l'aide de l'interface Web, voir « Configuration d'Active Directory avec le schéma standard via l'interface Web d'iDRAC6 ».

Importation du certificat SSL du micrologiciel iDRAC6

REMARQUE : Si le serveur Active Directory est défini pour authentifier le client lors de la phase d'initialisation d'une session SSL, vous devez également télécharger le certificat du serveur iDRAC6 sur le contrôleur de domaine d'Active Directory. Cette étape supplémentaire n'est pas nécessaire si Active Directory ne procède pas à l'authentification du client lors de la phase d'initialisation d'une session SSL.

Utilisez la procédure suivante pour importer le certificat SSL du micrologiciel iDRAC6 dans toutes les listes de certificats sécurisées de contrôleur de domaine.

REMARQUE : Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

REMARQUE : Si le certificat SSL du micrologiciel iDRAC6 est signé par une autorité de certification connue et que le certificat de cette autorité se trouve déjà dans la liste des autorités de certification racines de confiance du contrôleur de domaine, il n'est pas nécessaire d'effectuer la procédure ci-après.

Le certificat SSL iDRAC6 est le même que celui utilisé pour le serveur Web iDRAC6. Tous les contrôleurs iDRAC6 sont livrés avec un certificat auto-signé par défaut.

Pour télécharger le certificat SSL d'iDRAC6, exécutez la commande RACADM suivante :

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

1. Sur le contrôleur de domaine, ouvrez une fenêtre **Console MMC** et sélectionnez **Certificats**→ **Autorités de certification racines de confiance**.
2. Cliquez-droite sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
3. Cliquez sur **Suivant** et naviguez pour sélectionner le fichier de certificat SSL.

4. Installez le certificat SSL d'iDRAC6 dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

   Si vous avez installé votre propre certificat, assurez-vous que la CA qui signe votre certificat est dans la liste des **autorités de certification racines de confiance**. Si elle ne l'est pas, vous devez l'installer sur tous vos contrôleurs de domaine.

5. Cliquez sur **Suivant** et choisissez si vous voulez que Windows sélectionne automatiquement le magasin de certificats en fonction du type de certificat ou sélectionnez un magasin de votre choix.

6. Cliquez sur **Terminer** et cliquez sur **OK**.

Utilisation d'Active Directory pour ouvrir une session iDRAC6

Pour ouvrir une session iDRAC6 à l'aide d'Active Directory, utilisez l'une des solutions suivantes :

- Interface Web
- RACADM locale
- Console SSH ou telnet pour l'interface CLI SM-CLP

La syntaxe d'ouverture de session est la même pour les trois méthodes :

<nom d'utilisateur@domaine>

ou

*<domaine>**<nom d'utilisateur>* ou *<domaine>*/*<nom d'utilisateur>*

où *nom d'utilisateur* est une chaîne de caractères ASCII de 1 à 256 octets.

Les espaces blancs et les caractères spéciaux (comme \, / ou @) ne peuvent pas être utilisés pour le nom d'utilisateur ou le nom de domaine.

REMARQUE : Vous ne pouvez pas spécifier de noms de domaine NetBIOS, tels que *Amériques* car ces noms ne peuvent pas être résolus.

Si vous ouvrez une session à partir de l'interface Web et que vous avez configuré des domaines utilisateur, l'écran de connexion à l'interface Web répertorie tous les domaines utilisateur dans le menu déroulant, afin que vous puissiez en choisir un. Si vous sélectionnez un domaine utilisateur dans le menu déroulant , il vous suffit d'indiquer le nom utilisateur. Si vous sélectionnez **cet iDRAC**, vous pouvez toujours vous connecter en tant qu'utilisateur Active Directory, si vous utilisez la syntaxe d'ouverture de session décrite plus haut, dans la section « Utilisation d'Active Directory pour ouvrir une session iDRAC6 ».

Questions les plus fréquentes

Problèmes de connexion à Active Directory

L'ouverture de session Active Directory a échoué. Que dois-je faire ?

iDRAC6 fournit un outil de diagnostic dans l'interface Web.

1. À partir de l'interface Web, connectez-vous en tant qu'utilisateur local avec des privilèges d'administrateur.

2. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ **iDRAC**.

3. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur le sous-onglet **Active Directory**.

   La page **Configuration et gestion d'Active Directory** apparaît.

4. Faites défiler l'écran vers le bas, puis cliquer sur **Test Settings (Tester les paramètres)**.

   L'écran **Test Active Directory Settings** (Tester les paramètres d'Active Directory) s'affiche.

5. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Start Test (Lancer le test)**.

   iDRAC6 exécute les tests étape par étape, et affiche le résultat pour chaque étape. iDRAC6 génère également un résultat de test détaillé afin de vous aider à résoudre les problèmes éventuels.

   Si des problèmes persistent :

   a. Dans l'écran **Test Settings** (Tester les paramètres), cliquez sur le sous- onglet **Active Directory** pour revenir à l'écran **Configuration et gestion d'Active Directory**.

b. Faites dérouler l'écran vers le bas, puis cliquez sur **Configurer Active Directory**.

c. Modifiez votre configuration utilisateur, puis exécutez de nouveau le test, jusqu'à ce que l'utilisateur test passe avec succès l'étape d'autorisation.

J'ai activé la validation de certificat mais je ne parviens pas à ouvrir une session Active Directory. J'ai exécuté les diagnostics à partir de l'interface GUI et le résultat du test affiche un message d'erreur indiquant un problème de connexion LDAP :

```
ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.
(Vérifiez que le certificat CA approprié a été téléchargé dans iDRAC. Vérifiez également que la date iDRAC se situe dans la période de validité du certificat et que l'adresse de contrôleur de domaine définie dans iDRAC correspond au sujet du certificat de serveur Active Directory.)
```

D'où vient le problème et comment puis-je le corriger ?

Si la validation de certificat est activée, iDRAC6 utilise le certificat CA téléchargé pour vérifier le certificat du serveur de répertoires lorsque l'iDRAC6 établit une connexion SSL avec le serveur de répertoires. Les raisons les plus courantes de l'échec d'une validation de certificat sont les suivantes :

- La date de l'iDRAC6 ne se situe pas dans la période de validité du certificat de serveur ou du certificat CA. Vérifiez l'heure de l'iDRAC6 et la période de validité de votre certificat.
- Les adresses des contrôleurs de domaine définies dans iDRAC6 ne correspondent pas au nom de demandeur ou à l'autre nom de demandeur du certificat de serveur de répertoires.
  - Si vous possédez une adresse IP, reportez-vous à la section « L'adresse de contrôleur de domaine que j'utilise est une adresse IP et la validation du certificat a échoué. D'où vient ce problème ? ».
  - Si vous utilisez FQDN, assurez-vous que vous utilisez le FQDN du contrôleur de domaine, et non celui du domaine directement. Par exemple, saisissez nom serveur.exemple.com et *non* exemple.com.

Quels éléments dois-je vérifier si je ne parviens pas à ouvrir une session iDRAC6 à l'aide d'Active Directory ?

Tout d'abord, diagnostiquez le problème à l'aide de la fonction Test Settings (Tester les paramètres). Pour obtenir des instructions, consultez la section « L'ouverture de session Active Directory a échoué. Que dois-je faire ? »

Ensuite, corrigez le problème indiqué par les résultats du test. Pour plus d'informations, voir « Test de vos configurations ».

Les problèmes les plus courants sont expliqués dans cette section. Toutefois, en règle générale, il est conseillé de vérifier les points suivants :

1. Assurez-vous que vous utilisez le nom de domaine utilisateur correct pendant l'ouverture de session, et non le nom NetBIOS.
2. Si vous avez un compte utilisateur iDRAC6 local, ouvrez une session iDRAC6 à l'aide de vos références locales.
3. Vérifiez les paramètres suivants :
   a. Accédez à l'écran **Configuration et gestion d'Active Directory**. Sélectionnez **Système→ Accès à distance→ iDRAC**, cliquez sur l'onglet **Réseau/Sécurité**, puis sur le sous-onglet **Active Directory**.
   b. Vérifiez que la case **Active Directory Enabled (Active Directory activé)** est cochée.
   c. Si vous avez activé la validation de certificat, vérifiez que vous avez téléchargé le certificat racine Active Directory approprié dans iDRAC6. Le certificat s'affiche dans la zone **Active Directory CA Certificate (Certificat CA d'Active Directory)**. Vérifiez que l'heure de l'iDRAC6 se situe dans la période de validité du certificat CA.
   d. Si vous utilisez le schéma étendu, vérifiez que le nom **iDRAC** et le nom de domaine **iDRAC** correspondent à la configuration de votre environnement Active Directory.

      Si vous utilisez le schéma standard vérifiez que le **nom du groupe** et le **nom de domaine du groupe** correspondent à la configuration de votre environnement Active Directory.
   e. Accédez à l'écran Configuration réseau. Cliquez sur **Système→ Accès à distance→ iDRAC**, puis sur **Réseau/Sécurité**. Vérifiez que les paramètres du DNS sont corrects.
   f. Vérifiez les certificats SSL du contrôleur de domaine afin de vous assurer que l'heure de l'iDRAC6 se situe dans la période de validité du certificat.

Validation de certificat Active Directory

L'adresse de contrôleur de domaine que j'utilise est une adresse IP et la validation du certificat a échoué. D'où vient ce problème ?

Vérifiez le champ Demandeur ou Subject Alternative Name (autre nom du demandeur) de votre certificat de contrôleur de domaine. En règle générale, dans le champ Demandeur ou Subject Alternative Name (autre nom du demandeur), Active Directory utilise le nom d'hôte du certificat de contrôleur de domaine, et non l'adresse IP. Pour résoudre ce problème, procédez de l'une des manières suivantes :

- Configurez le nom d'hôte (FQDN) du contrôleur de domaine en tant qu'*adresse(s) de contrôleur de domaine* sur iDRAC6, afin qu'il corresponde au demandeur ou à l'autre nom du demandeur du certificat de serveur.
- Générez de nouveau le certificat de serveur pour qu'il utilise une adresse IP dans le champ Demandeur ou Subject Alternative Name (Autre nom du demandeur), afin qu'il corresponde à l'adresse IP définie dans iDRAC6.
- Désactivez la validation de certificat si vous choisissez de faire confiance à ce contrôleur de domaine sans validation de certificat lors de l'établissement d'une liaison SSL.

Pourquoi la validation de certificat est-elle activée par défaut dans iDRAC6 ?

iDRAC6 applique une sécurité stricte afin de vérifier l'identité du contrôleur de domaine auquel se connecte l'iDRAC6. Sans validation de certificat, le contrôleur de domaine pourrait être usurpé par un pirate informatique, et la connexion SSL pourrait être interceptée. Si vous choisissez de faire confiance à tous les contrôleurs de domaine dans la zone de sécurité, sans validation de certificat, vous pouvez désactiver cette option via l'interface GUI ou CLI.

Schéma étendu et standard

J'utilise un schéma étendu dans un environnement à plusieurs domaines. Comment dois-je configurer les adresses des contrôleurs de domaine ?

Utilisez le nom d'hôte (FQDN) ou l'adresse IP du contrôleur de domaine associé au domaine dans lequel réside l'objet iDRAC6.

Dois-je configurer des adresses de catalogue global ?

Si vous utilisez un schéma étendu, vous ne pouvez pas configurer des adresses de catalogue global, car celles-ci ne sont pas utilisées avec les schémas étendus.

Si vous utilisez un schéma standard ainsi que des utilisateurs et des groupes de rôles de différents domaines, vous devez configurer au moins une adresse de catalogue global. Dans ce cas, vous pouvez uniquement utiliser un groupe universel.

Si vous utilisez un schéma standard et que tous les utilisateurs et groupes de rôles se trouvent dans le même domaine, il n'est pas nécessaire de configurer des adresses de catalogue global.

Comment fonctionne la fonction d'interrogation du schéma standard ?

Tout d'abord, iDRAC6 se connecte aux adresses de contrôleur de domaine configurées. Si l'utilisateur et les groupes de rôles résident dans ce domaine, les privilèges sont conservés.

Si des adresses de contrôleur global sont configurées, iDRAC6 continue d'interroger le catalogue global. Si des privilèges supplémentaires sont extraits du catalogue global, ces privilèges sont accumulés.

Divers

L'iDRAC6 utilise-t-il toujours l'authentification « LDAP over SSL »?

Oui. L'intégralité du transport s'effectue via les ports sécurisés 636 et/ou 3269.

Au cours du *test des paramètres*, iDRAC6 lance une requête LDAP CONNECT (connexion LDAP), pour isoler le problème uniquement, mais ne lance pas de requête LDAP BIND (liaison LDAP) sur une connexion non sécurisée.

L'iDRAC6 prend-il en charge le nom NetBIOS ?

Non, pas dans cette version.

Retour à la page du sommaire

Retour à la page du sommaire

Visualisation de la configuration et de l'intégrité du serveur géré

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

---

Récapitulatif système

Cliquez sur **Système**→ **Propriétés**→ **Résumé** pour obtenir des informations sur l'enceinte principale du système et sur Integrated Dell Remote Access Controller.

Enceinte principale du système

Informations sur le système

Cette section de l'interface Web iDRAC6 fournit les informations de base suivantes sur le serveur géré :

- Description : le numéro de modèle ou le nom du serveur géré
- Version du BIOS : le numéro de version du BIOS du serveur géré
- Numéro de service : le numéro de service du serveur géré
- Nom d'hôte : le nom d'hôte DNS associé au serveur géré
- Nom du SE : le nom du système d'exploitation installé sur le serveur géré

Carte mezzanine d'E/S

Cette section de l'interface Web iDRAC6 fournit les informations suivantes sur les cartes mezzanines d'E/S installées sur le serveur géré :

- Connexion : énumère la ou les cartes mezzanines d'E/S installées sur le serveur géré
- Type de carte : le type physique de la carte mezzanine/connexion installée
- Nom du modèle : le numéro du modèle, le type ou la description de la ou des cartes mezzanines installées

Carte de stockage intégrée

Cette section de l'interface Web iDRAC6 fournit des informations sur la carte du contrôleur de stockage intégrée installée sur le serveur géré :

- Type de carte : affiche le nom du modèle de la carte de stockage installée

Reprise auto

Cette section de l'interface Web iDRAC6 détaille le mode actuel de fonctionnement de la fonctionnalité Récupération auto du serveur géré comme définie par OpenManage Server Administrator :

- Action de reprise : action à effectuer en cas de détection d'une défaillance ou d'une *suspension* du système. Les actions disponibles sont **Pas d'action**, **Réinitialisation matérielle**, **Mise hors tension** ou **Cycle d'alimentation**.
- Compte à rebours initial : le temps (en secondes) après lequel une suspension du système est détectée et auquel iDRAC6 effectue une action de récupération.
- Compte à rebours présent : la valeur actuelle (en secondes) du temporisateur de compte à rebours.

Integrated Dell Remote Access Controller 6 - Enterprise

Informations sur iDRAC6

Cette section de l'interface Web iDRAC6 fournit les informations suivantes sur iDRAC6 lui-même :

- Date/Heure : la date et l'heure actuelles (à compter de la dernière actualisation de la page) d'iDRAC6

- Version du micrologiciel : la version actuelle du micrologiciel iDRAC6 installé sur le serveur géré
- Micrologiciel mis à jour : la date et l'heure de la dernière mise à jour réussie du micrologiciel iDRAC6
- Version du matériel : le numéro de version de la carte à circuits imprimés planaire primaire du serveur géré
- Adresse IP : l'adresse IP associée à iDRAC6 (et non au serveur géré)
- Passerelle : l'adresse IP de la passerelle réseau configurée pour iDRAC6
- Masque de sous-réseau : le masque de sous-réseau TCP/IP configuré pour iDRAC6
- Adresse MAC : l'adresse MAC associée au contrôleur d'interface réseau LOM (LAN sur carte mère) d'iDRAC6
- DHCP activé : activé si iDRAC6 est défini pour chercher son adresse IP et les infos associées auprès d'un serveur DHCP
- Adresse DNS préférée 1 : définie sur le serveur DNS primaire actuellement actif
- Autre adresse DNS 2 : définie sur l'autre adresse du serveur DNS

REMARQUE : Ces informations sont également disponibles à **iDRAC**→ **Propriétés**→ **Informations iDRAC** .

Résumé WWN/MAC

Cliquez sur **Système**→ **Propriétés**→ **WWN/MAC** pour visualiser la configuration actuelle des cartes mezzanines d'E/S installées et la structure des réseaux associés. Si la fonctionnalité FlexAddress est activée, les adresses MAC persistantes assignées globalement (assignées au châssis) remplacent les valeurs câblées de chaque LOM.

Intégrité du système

Cliquez sur **Système**→ **Propriétés**→ **Intégrité** pour afficher des informations importantes sur l'intégrité d'iDRAC6 et des composants surveillés par iDRAC6. La colonne **Gravité** indique l'état de chaque composant. Pour une liste des icônes d'état et leur signification, voir Tableau 17-3. Cliquez sur le nom du composant dans la colonne **Composant** pour plus d'informations détaillées sur le composant

REMARQUE : Pour obtenir les informations sur le composant, vous pouvez également cliquer sur le nom du composant dans le panneau gauche de la fenêtre. Les composants restent visibles dans le panneau gauche, indépendamment de l'onglet/l'écran sélectionné.

Carte iDRAC6

L'écran **Informations sur iDRAC6** énumère plusieurs détails importants sur iDRAC6, comme la condition d'intégrité, le nom, la révision du micrologiciel et les paramètres réseau. Pour obtenir des détails supplémentaires, cliquez sur l'onglet approprié en haut de l'écran.

CMC

L'écran **CMC** affiche la condition d'intégrité, la révision du micrologiciel et l'adresse IP de Chassis Management Controller. Vous pouvez également lancer l'interface Web du CMC en cliquant sur le bouton **Lancer l'interface Web du CMC**. Consultez le *Guide d'utilisation du micrologiciel Chassis Management Controller*.

Piles

L'écran **Piles** affiche la condition et les valeurs de la pile bouton de la carte système qui permet de stocker les données de configuration de l'horloge temps réel (RTC) et CMOS du système géré.

Températures

L'écran **Informations sur les sondes de température** affiche la condition et les mesures de la sonde de température ambiante intégrée. Les seuils de température minimum et maximum correspondant à l'état *avertissement* ou *défaillance* sont affichés avec l'état d'intégrité actuel de la sonde.

Tensions

L'écran **Informations sur les sondes de tension** affiche la condition et la mesure des sondes de tension, donnant des informations telles que la condition des capteurs de noyau CPU et de pôle de tension intégrés.

REMARQUE : Selon le modèle de votre serveur, les seuils de température des états *avertissement* ou *défaillance* et/ou l'état d'intégrité de la sonde peuvent ne pas s'afficher.

Surveillance de l'alimentation

L'écran **Surveillance de l'alimentation** vous permet d'afficher les informations suivantes relatives à la surveillance et aux statistiques d'alimentation :

- Surveillance de l'alimentation : affiche l'alimentation consommée (en watts) par le serveur telle que communiquée par le moniteur de courant de la carte système.
- Statistiques de suivi de l'alimentation : affiche des informations sur l'alimentation consommée par le système depuis la dernière réinitialisation de l'**Heure de début de la mesure**.
- Statistiques de crête : affiche des informations sur l'alimentation de crête consommée par le système depuis la dernière réinitialisation de l'**Heure de début de la mesure**.

UC

L'écran **Informations UC** indique l'intégrité de chaque UC sur le serveur géré. Cet état d'intégrité est un cumul de plusieurs tests thermiques, d'alimentation et fonctionnels individuels.

POST

L'écran **Code du POST** affiche le dernier code du POST du système (au format hexadécimal) avant le démarrage du système d'exploitation du serveur géré.

Intégrité div

L'écran **Intégrité div** permet d'accéder aux journaux système suivants :

- Journal des événements système (SEL) : affiche les événements critiques qui se produisent sur le système géré.
- Post code : affiche le dernier post code du système (au format hexadécimal) avant l'amorçage du système d'exploitation du serveur géré.
- Dernière panne : affiche l'écran et l'heure de la dernière panne.
- Saisie de l'amorçage : permet de lire les trois derniers écrans d'amorçage.

REMARQUE : Ces informations sont également disponibles dans **Système**→ **Propriétés**→ **Journaux**.

Retour à la page du sommaire

Retour à la page du sommaire

Surveillance et gestion de l'alimentation

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Les systèmes Dell™ PowerEdge™ intègrent de nombreuses nouvelles fonctionnalités améliorées de gestion de l'alimentation. La plateforme entière, du matériel au micrologiciel jusqu'au logiciel Systems Management, a été conçue dans une optique d'efficacité, de surveillance et de gestion de l'alimentation.

Les systèmes PowerEdge fournissent de nombreuses fonctionnalités pour la surveillance et la gestion de l'alimentation :

- **Surveillance de l'alimentation :** iDRAC6 recueille un historique des mesures d'alimentation et calcule les moyennes, les pics, etc. L'interface Web iDRAC6 vous permet d'afficher les informations dans l'écran **Surveillance de l'alimentation**. Vous pouvez également afficher les informations sous forme de graphique en cliquant sur **Afficher le graphique** au bas de l'écran **Surveillance de l'alimentation**. Pour de plus amples informations, consultez la section « Contrôle de l'alimentation ».
- **Allocation de l'alimentation :** au démarrage, l'inventaire du système permet de calculer l'allocation de l'alimentation du système dans la configuration actuelle. Pour plus d'informations, voir «Surveillance de l'alimentation».
- **Contrôle de l'alimentation :** iDRAC6 vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance sur le système géré. Pour plus d'informations, voir «Contrôle de l'alimentation».

Configuration et gestion de l'alimentation

Vous pouvez utiliser l'interface Web iDRAC et l'interface de ligne de commande (CLI) RACADM et configurer les contrôles de l'alimentation sur le système PowerEdge. Vous pouvez notamment :

- Afficher la condition de l'alimentation du serveur. Voir «Affichage de la surveillance de l'alimentation».
- Afficher des informations sur l'allocation de l'alimentation du serveur, y compris la consommation électrique potentielle minimale et maximale. Voir « Affichage de l'allocation de l'alimentation ».
- Afficher le seuil d'allocation de l'alimentation du serveur. Voir « Affichage du seuil d'allocation de l'alimentation ».
- Exécuter des opérations de contrôle de l'alimentation sur le serveur (par exemple, mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation). Voir « Exécution d'opérations de contrôle de l'alimentation sur le serveur ».

Surveillance de l'alimentation

iDRAC6 surveille la consommation électrique des serveurs PowerEdge en continu. iDRAC6 calcule les valeurs d'alimentation suivantes et fournit les informations via son interface Web ou la CLI RACADM :

- Alimentation cumulée
- Alimentation moyenne, minimale et maximale
- Consommation électrique (également affichée dans des graphiques dans l'interface Web)
- Seuils d'allocation de l'alimentation

Affichage de la surveillance de l'alimentation

Utilisation de l'interface Web

Pour afficher les données sur la surveillance de l'alimentation :

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Surveillance de l'alimentation**.

   L'écran **Surveillance de l'alimentation** apparaît, affichant les informations suivantes :

Surveillance de l'alimentation

- **Condition** : une **coche verte** indique que la condition d'alimentation est normale, **Avertissement** indique qu'une alerte d'avertissement a été émise et **Grave** indique qu'une alerte d'échec a été émise.
- **Nom de la sonde** : niveau système de la carte système. Cette description indique que la sonde est surveillée du fait de son emplacement dans le

système.

- **Mesure** : la consommation électrique actuelle en watts.

Intensité

- **Emplacement** : courant du moniteur de courant de la carte système
- **Mesure** : la consommation électrique actuelle en ampères

Statistiques de consommation de puissance

- Statistique :
  - **Alimentation cumulée du système** affiche la consommation d'énergie cumulée actuelle (en KWh) du serveur. La valeur représente l'énergie totale utilisée par le système. Vous pouvez réinitialiser cette valeur sur 0 en cliquant sur **Réinitialiser** à la fin de la ligne du tableau.
  - **Alimentation maximale du système** spécifie la valeur maximale du système en watts dans l'intervalle indiqué par **Heure de début de la mesure** et **Heure actuelle de la mesure**. Vous pouvez réinitialiser cette valeur sur 0 en cliquant sur **Réinitialiser** à la fin de la ligne du tableau.
  - **Ampérage maximal du système** spécifie l'ampérage maximal du système dans l'intervalle indiqué par **Heure de début de la mesure** et **Heure actuelle de la mesure**. Vous pouvez réinitialiser cette valeur sur 0 en cliquant sur **Réinitialiser** à la fin de la ligne du tableau.
- **Heure de début de la mesure** affiche la date et l'heure enregistrées lorsque la dernière valeur relative à la consommation d'énergie du système a été effacée et que le nouveau cycle de mesure a débuté. Pour les statistiques **Alimentation cumulée du système**, **Ampérage maximal du système** et **Alimentation maximale du système**, vous pouvez réinitialiser chaque valeur sur 0 en cliquant sur **Réinitialiser** à la fin de la ligne du tableau ; toutefois, elle est conservée pendant une réinitialisation du système ou une opération d'échec du CMC.
- **Heure actuelle de la mesure** pour **Alimentation cumulée du système** affiche la date et l'heure actuelles lorsque la consommation d'énergie du système a été calculée pour l'affichage. Pour **Ampérage maximal du système** et **Alimentation maximale du système**, les champs **Heure maximale** affichent l'heure à laquelle ces pics se sont produits.
- **Mesure** : la quantité d'alimentation (en KWh) utilisée depuis le démarrage du compteur.

REMARQUE : Les statistiques de suivi de l'alimentation sont conservées sur l'ensemble des réinitialisations du système et reflètent ainsi toute l'activité dans l'intervalle entre les heures de début et de fin déclarées. Le bouton **Réinitialiser les pics max** réinitialise la valeur des statistiques maximale. Dans le tableau suivant, les données sur la consommation électrique ne sont pas conservées sur l'ensemble des réinitialisations du système et reviendront ainsi à la valeur des statistiques maximale. Les valeurs d'alimentation affichées correspondent à des moyennes cumulées sur l'intervalle de temps respectif (minute, heure, jour et semaine précédents). Étant donné que les intervalles entre l'heure de début et l'heure de fin peuvent différer de ceux des statistiques de suivi de l'alimentation, les valeurs d'alimentation maximales (Pic max en watts par opposition à Consommation électrique max) peuvent différer.

Consommation de puissance

- **Consommation électrique moyenne** : moyenne sur la minute précédente, l'heure précédente, le jour précédent et la semaine précédente.
- **Consommation électrique max** et **Consommation électrique min** : les consommations électriques maximale et minimale observées dans l'intervalle de temps donné.
- **Heure d'alimentation max** et **Heure d'alimentation min** : les heures (par minute, heure, jour et semaine) auxquelles se sont produites les consommations électriques maximale et minimale.

Afficher le graphique

Cliquez sur **Afficher le graphique** pour afficher des graphiques illustrant la consommation électrique iDRAC6 en watts au cours de la dernière heure, des dernières 24 heures, des trois derniers jours et de la dernière semaine. Utilisez le menu déroulant fourni au-dessus du graphique pour sélectionner la période.

REMARQUE : Chaque point de données tracé sur les graphiques représente la moyenne des mesures sur une période de 5 minutes. En conséquence de quoi, les graphiques ne reflèteront peut-être pas les brèves fluctuations d'alimentation ou de consommation électrique.

Allocation d'énergie

iDRAC6 peut être configuré pour appliquer les limites de seuil d'alimentation minimale et maximale, telles que définies par le CMC, pour la configuration actuelle du système. L'écran **Allocation de l'alimentation** affiche ces limites de seuil d'alimentation, qui couvrent la plage des consommations électriques en CA qu'un système à seuil soumis à une lourde charge de travail présentera au centre de données. Ces limites ne sont pas configurables.

Affichage de l'allocation de l'alimentation

Le serveur fournit des aperçus de la condition d'allocation de l'alimentation du sous-système d'alimentation dans l'écran **Informations sur l'allocation de l'alimentation**.

Utilisation de l'interface Web

REMARQUE : Vous devez disposer d'un droit **administratif** pour effectuer des actions de gestion de l'alimentation.

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système.**
3. Cliquez sur l'onglet **Gestion de l'alimentation**, puis sur **Allocation de l'alimentation**.

   L'écran **Informations sur l'allocation de l'alimentation** apparaît.

Le tableau **Informations sur l'allocation de l'alimentation** affiche les limites minimale et maximale des seuils d'alimentation pour la configuration système actuelle. Ces limites couvrent la plage des consommations électriques en CA qu'un système à seuil soumis à une lourde charge de travail présentera au centre de données.

- **Consommation électrique potentielle minimale** représente la valeur Seuil d'allocation de l'alimentation la plus basse.
- **Consommation électrique potentielle maximale** représente la valeur Seuil d'allocation de l'alimentation la plus haute. Cette valeur représente également la consommation électrique maximale absolue de la configuration système actuelle.

Utilisation de RACADM

Sur un noeud géré, ouvrez une interface de ligne de commande et tapez :

```
racadm getconfig -g cfgServerPower
```

REMARQUE : Pour plus d'informations concernant cfgServerPower, y compris le détail des résultats renvoyés, consultez la section « cfgServerPower ».

Affichage du seuil d'allocation de l'alimentation

Le seuil d'allocation de l'alimentation, s'il est activé, applique les limites d'alimentation pour le système. Les performances du système sont ajustées dynamiquement pour maintenir la consommation électrique près du seuil spécifié.

REMARQUE : Le seuil d'allocation de l'alimentation est en lecture seule et ne peut pas être activé ou configuré dans iDRAC6.

La consommation électrique réelle peut être inférieure pour les charges de travail légères et excéder momentanément le seuil jusqu'à ce que les performances aient été ajustées.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système.**
3. Cliquez sur l'onglet **Gestion de l'alimentation**, puis sur **Allocation de l'alimentation**.

   L'écran **Informations sur l'allocation de l'alimentation** apparaît.
4. Cliquez sur **Seuil d'allocation de l'alimentation**.

Le tableau **Seuil d'allocation de l'alimentation** affiche les informations sur les limites d'alimentation pour le système :

- **Activé** indique si le système applique le seuil d'allocation de l'alimentation.
- **Seuil en watts** et **Seuil en BTU/h** affichent les limites en watts et en BTU/h, respectivement.
- **Pourcentage du seuil** affiche le pourcentage de la plage d'alimentation.

Utilisation de RACADM

Sur un noeud géré, ouvrez une interface de ligne de commande et tapez :

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts <valeur du plafond d'alimentation en watts>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr <valeur du plafond d'alimentation en BTU/h>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent <valeur du plafond d'alimentation en %>
```

REMARQUE : Pour plus d'informations concernant cfgServerPower, y compris le détail des résultats renvoyés, consultez la section « cfgServerPower ».

Contrôle de l'alimentation

iDRAC6 vous permet d'effectuer à distance une mise sous tension, une réinitialisation, un arrêt normal, une interruption non masquable (NMI) ou un cycle d'alimentation. Utilisez l'écran **Contrôle de l'alimentation** pour réaliser un arrêt méthodique via le système d'exploitation lors du redémarrage et des mises sous et hors tension.

Exécution d'opérations de contrôle de l'alimentation sur le serveur

REMARQUE : Pour réaliser des actions de gestion de l'alimentation, vous devez disposer du droit d'**administrateur de contrôle du châssis.**

iDRAC6 vous permet d'effectuer à distance une mise sous tension, une réinitialisation, un arrêt normal, une NMI ou un cycle d'alimentation.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **Power Management** (Gestion de l'alimentation).

   L'écran **Contrôle de l'alimentation** s'affiche.
4. Sélectionnez l'une des **Opérations de contrôle de l'alimentation** suivantes en cliquant sur son bouton radio :
   - **Mettre le système sous tension** met le serveur sous tension (équivaut à appuyer sur le bouton d'alimentation quand le serveur est hors tension). Cette option est désactivée si le système est déjà sous tension.
   - **Mettre le système hors tension** met le serveur hors tension. Cette option est désactivée si le système est déjà hors tension.
   - **NMI (interruption non masquable)** génère une NMI pour interrompre le fonctionnement du système. Une NMI envoie une interruption de niveau élevé au système d'exploitation, qui par conséquent interrompt le fonctionnement 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. L'arrêt normal nécessite que le système d'exploitation prenne en charge l'interface ACPI (Advanced Configuration and Power Interface [interface de configuration et d'alimentation avancée]) afin de contrôler la gestion de l'alimentation système.
   - **Réinitialiser le système (démarrage à chaud)** redémarre le système sans le mettre hors tension. Cette option est désactivée si le système est déjà hors tension.
   - **Cycle d'alimentation du système (démarrage à froid)** met sous tension, puis redémarre le système. Cette option est désactivée si le système est déjà hors tension.
5. Cliquez sur **Appliquer**.

   Une boîte de dialogue vous demande de confirmer l'opération.
6. Cliquez sur **OK** pour exécuter l'action de gestion de l'alimentation que vous avez sélectionnée.

Utilisation de RACADM

Ouvrez une console textuelle de l'interface de ligne de commande ouverte du noeud géré sur le serveur, ouvrez une session, puis tapez :

```
racadm serveraction <action>
```

où `<action>` a pour valeur `powerup`, `powerdown`, `powercycle`, `hardreset` ou `powerstatus`.

REMARQUE : Pour plus d'informations concernant serveraction, y compris le détail des résultats renvoyés, consultez la section « serveraction ».

Retour à la page du sommaire

Retour à la page du sommaire

Configuration et utilisation des communications série sur le LAN

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Communications série sur le LAN (SOL) est une fonctionnalité IPMI qui permet de rediriger sur le réseau de gestion Ethernet hors bande dédié iDRAC les données de la console textuelle d'un serveur géré, qui seraient traditionnellement envoyées vers le port E/S série. La console hors bande SOL permet aux administrateurs système de gérer à distance la console textuelle du serveur lame depuis n'importe quel emplacement possédant un accès réseau. Les avantages de SOL sont les suivants :

- d'accéder à distance aux systèmes d'exploitation sans délai ;
- diagnostiquer les systèmes hôte sur Emergency Management Services (EMS) ou Special Administrator Console (SAC) pour Windows ou dans un environnement Linux ;
- visualiser la progression d'un serveur lame pendant le POST et renconfigurer le programme de configuration du BIOS (pendant la redirection vers un port série).

Activation des communications série sur le LAN dans le BIOS

Pour configurer le serveur pour les communications série sur le LAN, vous devez suivre les étapes de configuration expliquées en détail ci-dessous.

1. Configurer les communications série sur le LAN dans le BIOS (désactivé par défaut)
2. Configurer iDRAC6 pour les communications série sur le LAN
3. Sélectionner une méthode pour initialiser les communications série sur le LAN (SSH, Telnet, proxy SOL ou IPMItool)
4. Configurer le SE pour SOL

La communication série est **désactivée** par défaut dans le BIOS. Pour rediriger les données de la console textuelle hôte vers les communications série sur le LAN, vous devez activer la redirection de console via COM1. Pour changer le paramètre du BIOS, effectuez les étapes suivantes :

1. Démarrez le serveur géré.
2. Appuyez sur <F2> pour accéder à l'utilitaire de configuration du BIOS pendant le POST.
3. Défilez vers le bas jusqu'à Communication série et appuyez sur <Entrée>.

   Dans la fenêtre contextuelle, la liste des communications série affichée comprend les options suivantes :

   - Éteint
   - Activé sans redirection de console
   - Activé avec redirection de console via COM1

   Utilisez les touches fléchées pour naviguer entre les options.
4. Assurez-vous qu'**Activé avec redirection de console via COM1** est activé.
5. Assurez-vous que **Débit en bauds à sécurité intégrée** est identique au débits en bauds SOL qui est configuré sur l'iDRAC. La valeur par défaut du débit en bauds à sécurité intégrée et du débit en bauds SOL de l'iDRAC est 115,2 kb/s.
6. Activez la **Redirection après démarrage** (la valeur par défaut est DÉSACTIVÉ). Cette option active la redirection SOL du BIOS à chaque redémarrage.
7. Enregistrez les modifications et quittez.

   Le serveur géré redémarre.

Configuration des communications série sur le LAN dans l'interface utilisateur Web iDRAC6

1. Ouvrez l'écran **Configuration des communications série sur le LAN** en sélectionnant **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Communications série sur le LAN**.

2. Assurez-vous que l'option **Activation des communications série sur le LAN** est sélectionnée (activée). Elle est activée par défaut.

3. Mettez à jour le débit en bauds SOL IPMI en sélectionnant une vitesse de données dans le menu déroulant **Débit en bauds**. Les options sont 19,2 kb/ s, 57,6 kb/s et 115,2 kb/s. La valeur par défaut est 115,2 kb/s.

   REMARQUE : Assurez-vous que le débit en bauds SOL est identique au débit en bauds à sécurité intégrée qui a été défini dans le BIOS.

4. Cliquez sur **Appliquer** si vous avez apporté des modifications.

Tableau 9-1. Paramètres de configuration des communications série sur le LAN

Paramètre	Description
Activer la connexion série sur le réseau local	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 9-2. Boutons de l'écran 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 l'écran **Configuration des communications série sur le LAN.**
Paramètres avancés	Ouvre l'écran **Paramètres avancés de la configuration des communications série sur le LAN**.
Appliquer	Fournit les nouveaux paramètres que vous créez lors de l'affichage de l'écran **Configuration des communications série sur le LAN**.

5. Modifiez la configuration dans l'écran **Paramètres avancés**, le cas échéant. Dell vous recommande d'utiliser les valeurs par défaut. **Paramètres avancés** vous permet d'ajuster les performances SOL en modifiant les valeurs **Intervalle d'accumulation des caractères** et **Seuil d'envoi des caractères**. Pour des performances optimales, utilisez les paramètres par défaut : 10 millisecondes et 250 caractères, respectivement.

Tableau 9-3. Paramètres avancés de la configuration des communications série sur le LAN

Paramètre	Description
Intervalle d'accumulation des caractères	Le temps type pendant lequel iDRAC6 attend avant d'envoyer un paquet de données SOL partiel. Ce paramètre est spécifié en millisecondes et incrémente de 10 millisecondes.
Seuil d'envoi des caractères	Spécifie le nombre de caractères par paquet de données SOL. Dès que le nombre de caractères acceptés par iDRAC6 est supérieur ou égal à la valeur Seuil d'envoi des caractères, iDRAC6 commence la transmission des paquets de données SOL qui contiennent un nombre de caractères inférieur ou égal à la valeur Seuil d'envoi des caractères. Si un paquet contient un nombre de caractères inférieur à cette valeur, il est défini comme étant un paquet de données SOL partiel.

REMARQUE : Si vous remplacez ces valeurs par des valeurs inférieures, les performances de la fonctionnalité de redirection de console de SOL peuvent être diminuées. En outre, la session SOL doit attendre de recevoir un accusé de réception pour chaque paquet avant d'envoyer le paquet suivant. Les performances sont ainsi considérablement réduites.

Tableau 9-4. Boutons de l'écran 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 l'écran **Paramètres avancés de la configuration des communications série sur le LAN**.
Appliquer	Enregistre les nouveaux paramètres que vous créez pendant l'affichage de l'écran **Paramètres avancés de la configuration des communications série sur le LAN**.
Retour à la page Configuration de la communication série sur LAN	Renvoie l'utilisateur à l'écran **Configuration des communications série sur le LAN**.

6. Configurez SSH/Telnet pour SOL dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services**.

   REMARQUE : Chaque serveur lame prend en charge une seule session SOL active via le protocole SSH ou Telnet.

   REMARQUE : Le protocole SSH est activé par défaut. Le protocole Telnet est désactivé par défaut.

7. Cliquez sur **Services** pour ouvrir l'écran **Configuration SSH et Telnet**.

REMARQUE : Les programmes SSH et Telnet permettent d'accéder à une machine distante.

8. Cliquez sur **Activer** sur **SSH** ou **Telnet**, selon les besoins.
9. Cliquez sur **Appliquer**.

REMARQUE : SSH est une méthode recommandée car il offre une sécurité accrue et des mécanismes de cryptage.

REMARQUE : Une session SSH/Telnet peut durer indéfiniment pour autant que la valeur du délai d'attente est définie sur 0. La valeur du délai d'attente par défaut est de **1800 secondes**.

10. Activez l'interface hors bande iDRAC6 (IPMI sur LAN) en sélectionnant **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Réseau**.
11. Activez l'option **IPMI sur LAN** sous **Paramètres LAN IPMI**. **La fonctionnalité IPMI sur LAN** est désactivée par défaut.
12. Cliquez sur **Appliquer**.

Utilisation des communications série sur le LAN (SOL)

Cette section indique plusieurs méthodes d'initialisation d'une session de communications série sur le LAN incluant un programme Telnet, un client SSH, IPMItool et proxy SOL. La fonctionnalité Communications série sur le LAN a pour objectif de rediriger le port série du serveur géré via iDRAC6 dans la console de votre station de gestion.

Modèle pour rediriger SOL sur Telnet ou SSH

Client Telnet (port 23)/SSH (port 22) ←→Connexion WAN ←→Serveur iDRAC6

L'implémentation SOL sur SSH/Telnet basée sur IPMI permet d'éliminer la nécessité de recourir à un utilitaire supplémentaire car la conversion série vers le réseau se produit au sein d'iDRAC. La console SSH ou Telnet 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-. La console série est automatiquement redirigée vers votre console SSH ou Telnet. La redirection SOL peut ensuite être démarrée à partir de la cible **/system/sol1**.

Consultez la section « Installation de clients Telnet ou SSH » pour obtenir plus d'informations sur l'utilisation de clients Telnet et SSH avec iDRAC.

Modèle pour le proxy SOL

Client Telnet (port 623) ←→Connexion WAN ←→Proxy SOL ←→ Serveur iDRAC6

Lorsque le proxy SOL communique avec le client Telnet sur une station de gestion, il utilise le protocole TCP/IP. Le proxy SOL communique toutefois avec iDRAC6 du système géré sur le protocole RMCP/IPMI/SOL, qui est un protocole basé sur UDP. Ainsi, si vous communiquez avec iDRAC6 de votre système géré depuis le proxy SOL sur une connexion WAN, les performances du réseau peuvent être compromises. Le modèle d'utilisation recommandé consiste à avoir le proxy SOL et le serveur iDRAC6 sur le même LAN. La station de gestion disposant du client Telnet peut alors se connecter au proxy SOL sur une connexion WAN. Dans ce modèle d'utilisation, le proxy SOL fonctionne comme vous le souhaitez.

Modèle pour rediriger SOL sur IPMItool

IPMItool ←→ Connexion WAN ←→ Serveur iDRAC6

L'utilitaire SOL basé sur IPMI (IPMItool) utilise le protocole RMCP+ livré au port 623 à l'aide de datagrammes UDP. iDRAC6 exige que cette connexion RMCP+ soit cryptée. La clé de cryptage (clé KG) doit contenir des caractères zéro ou NULL qui peuvent être configurés dans l'interface utilisateur Web iDRAC6 ou dans l'utilitaire de configuration iDRAC6. Vous pouvez également effacer la clé de cryptage en appuyant sur la touche Retour afin qu'iDRAC6 fournisse des caractères NULL comme clé de cryptage par défaut. RMCP+ offre comme avantage une authentification améliorée, des contrôles de l'intégrité des données, le cryptage et la capacité d'exécuter plusieurs types de charge utile. Consultez la section « Utilisation de SOL sur IPMItool » ou le site Web d'IPMItool pour plus d'informations : **http://ipmitool.sourceforge.net/manpage.html**.

Déconnexion d'une session SOL dans SM-CLP

Lorsque vous utilisez les protocoles SSH ou Telnet pour accéder à la fonctionnalité Communications série sur le LAN, vous devez tout d'abord vous connecter au service SM-CLP d'iDRAC, duquel vous lancerez la session SOL avec une commande SM-CLP (`start /system1/sol1`). Ainsi, les utilisateurs souhaitant se déconnecter d'une session SOL doivent d'abord terminer la session SOL depuis SM-CLP.

Les commandes de déconnexion d'une session SOL sont orientées utilitaire. Lisez attentivement cette section. C'est seulement lorsqu'une session SOL est complètement terminée que vous pouvez quitter l'utilitaire.

Lorsque vous êtes prêt à quitter la redirection SOL depuis SM-CLP, appuyez sur <Entrée>, <Échap>, puis <t> (appuyez sur ces touches dans l'ordre, l'une après l'autre). La session SOL se ferme.

REMARQUE : Si une session SOL n'est pas fermée correctement dans l'utilitaire, d'autres sessions SOL peuvent ne pas être disponibles. Pour résoudre cette situation, vous devez supprimer la console SMASH de l'interface utilisateur Web sous **Système**→**Accès à distance**→**iDRAC**→**Réseau/Sécurité**→**Sessions**.

Utilisation de SOL sur PuTTY

Pour démarrer SOL à partir de PuTTY sur une station de gestion Windows, suivez les étapes ci-dessous :

REMARQUE : Si nécessaire, vous pouvez modifier le délai d'attente SSH/Telnet par défaut dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services**.

1. Connectez-vous à iDRAC6 avec la commande suivante à l'invite de commande :

   ```
   putty.exe [-ssh | -telnet] <lnom d'ouverture de session>@<adresse-ip-DRAC> <numéro de port>
   ```

REMARQUE : Le numéro de port est facultatif. Il est requis uniquement lorsqu'il est réattribué.

2. Saisissez la commande suivante dans l'invite SM-CLP pour démarrer SOL :

   ```
   start /system1/sol1
   ```

   REMARQUE : Cette commande vous connecte au port série du serveur géré. Vous n'avez plus accès aux commandes SM-CLP. Vous ne pouvez pas revenir dans SM-CLP lorsque vous avez démarré SOL. Vous devez quitter la session SOL à l'aide de la séquence de commandes détaillée à la section « Déconnexion d'une session SOL dans SM-CLP » et démarrer une nouvelle session pour pouvoir utiliser SM-CLP.

Utilisation de SOL sur Telnet avec Linux

Pour démarrer SOL à partir de Telnet sur une station de gestion Linux, suivez ces étapes :

REMARQUE : Si nécessaire, vous pouvez modifier le délai d'attente Telnet par défaut dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services**.

1. Démarrez un environnement.

2. Connectez-vous à iDRAC6 à l'aide de la commande suivante :

   ```
   telnet <adresse IP iDRAC>
   ```

   REMARQUE : Si vous avez remplacé le numéro de port par défaut (port 23) du service Telnet par un autre numéro de port, ajoutez le numéro de port à la fin de la commande telnet.

3. Saisissez le nom d'utilisateur et le mot de passe d'iDRAC6 afin de vous connecter à SM-CLP iDRAC6.

4. Saisissez la commande suivante dans l'invite SM-CLP pour démarrer SOL :

   ```
   start /system1/sol1
   ```

5. Pour quitter une session SOL depuis Telnet sous Linux, appuyez sur <Ctrl>+] (maintenez la touche Ctrl enfoncée, appuyez sur la touche représentant un crochet droit, puis relâchez). Une invite Telnet s'affiche. Tapez `quit` pour quitter Telnet.

Utilisation de SOL sur OpenSSH avec Linux

OpenSSH est un utilitaire open source permettant d'utiliser le protocole SSH. Pour démarrer SOL à partir de OpenSSH sur une station de gestion Linux, suivez les étapes suivantes :

REMARQUE : Si nécessaire, vous pouvez modifier le délai d'attente de la session SSH par défaut dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services**.

1. Démarrez un environnement.

2. Connectez-vous à iDRAC6 à l'aide de la commande suivante :

   ```
   ssh <adresse-ip-iDRAC> -l <nom d'ouverture de session>
   ```

3. Saisissez la commande suivante dans l'invite SM-CLP pour démarrer SOL :

   ```
   start /system1/sol1
   ```

   REMARQUE : Cette commande vous connecte au port série du serveur géré. Vous n'avez plus accès aux commandes SM-CLP. Vous ne pouvez pas revenir dans SM-CLP lorsque vous avez démarré SOL. Vous devez quitter la session SOL (reportez-vous à la section « Déconnexion d'une session SOL dans SM-CLP » pour fermer une session SOL active) et démarrer une nouvelle session pour pouvoir utiliser SM-CLP.

Utilisation de SOL sur IPMItool

Le DVD *Dell Systems Management Tools and Documentation* fournit IPMItool, qui peut être installé sur divers systèmes d'exploitation. Pour démarrer SOL avec IPMItool sur une station de gestion, suivez les étapes ci-dessous :

REMARQUE : Si nécessaire, vous pouvez modifier le délai d'attente SOL par défaut dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services**.

1. Localisez IPMItool.exe dans le répertoire approprié.

   Le chemin par défaut pour Windows est **C:\Program Files\Dell\SysMgt\bmc**.

2. Assurez-vous que la **Clé de cryptage** ne comporte que des zéros dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Réseau**→ **Paramètres LAN IPMI**.

3. Saisissez la commande suivante dans l'invite de commande Windows ou dans l'invite d'environnement Linux pour démarrer SOL depuis iDRAC :

   ```
   ipmitool -H <adresse-ip-iDRAC> -I lanplus -U <nom d'ouverture de session> -P <mot de passe d'ouverture de session> sol activate
   ```

   Cette commande vous connecte au port série du serveur géré.

4. Pour quitter une session SOL depuis IPMItool, appuyez sur <~> et sur <.> (appuyez sur la touche tilde et sur la touche point dans l'ordre, l'une après l'autre). La session SOL se ferme.

   REMARQUE : Si un utilisateur ne termine pas la session SOL correctement, tapez la commande suivante pour redémarrer iDRAC. Laissez 1 à 2 minutes à iDRAC6 pour terminer son démarrage. Pour plus d'informations, voir « Présentation de la sous-commande RACADM ».

   ```
   racadm racreset
   ```

Ouverture de SOL avec le proxy SOL

Le proxy des communications série sur le LAN (proxy SOL) est un démon Telnet qui permet une administration basée sur le LAN des systèmes distants à l'aide des protocoles de communications série sur le LAN (SOL) et IPMI. Toute application client Telnet standard, comme HyperTerminal sous Microsoft Windows ou Telnet sous Linux, peut servir à accéder aux fonctionnalités du démon. Le SOL peut être utilisé dans le mode de menu ou le mode de commande. Le protocole SOL couplé à la redirection de console du BIOS du système distant permet aux administrateurs d'afficher et de modifier à distance les paramètres BIOS d'un système géré sur un LAN. La console série Linux et les interfaces de Microsoft EMS/SAC sont aussi accessibles via le LAN à l'aide des communications SOL.

REMARQUE : Toutes les versions du système d'exploitation Windows comprennent le logiciel d'émulation de terminal HyperTerminal. Cependant, la version comprise ne fournit pas beaucoup de fonctions requises pendant la redirection de console. À la place, vous pouvez utiliser tout logiciel d'émulation de terminal qui prend en charge le mode d'émulation VT100 ou ANSI. Un exemple d'émulateur de terminal complet VT100 ou ANSI qui prend en charge la redirection de console sur votre système est HyperTerminal Private Edition 6.1 ou version ultérieure.

REMARQUE : Consultez le Guide d'utilisation de votre système pour obtenir des informations supplémentaires sur la redirection de console, y compris les spécifications logicielles et matérielles, ainsi que des instructions pour configurer les systèmes hôtes et clients afin d'utiliser la redirection de console.

REMARQUE : Les paramètres HyperTerminal et Telnet doivent être cohérents avec les paramètres du système géré. Par exemple, les modes Débits en bauds et Terminal doivent correspondre.

REMARQUE : La commande Telnet Windows exécutée à partir d'une invite MS-DOS® prend en charge l'émulation de terminal ANSI et le BIOS doit être configuré pour l'émulation ANSI pour afficher correctement tous les écrans.

Avant d'utiliser le proxy SOL

Avant d'utiliser le proxy SOL, reportez-vous au *Guide d'utilisation des utilitaires du contrôleur de gestion de la carte mère* pour apprendre à configurer vos stations de gestion. Par défaut, l'utilitaire de gestion du contrôleur BMC est installé dans le répertoire suivant sur les systèmes d'exploitation Windows :

```
C:\Program Files\Dell\SysMgt\bmc
```

Le programme d'installation copie les fichiers dans les emplacements suivants sur les systèmes d'exploitation Linux Enterprise :

```
/etc/init.d/SOLPROXY.cfg

/etc/SOLPROXY.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/ipmish
```

Initiation de la session du proxy SOL

Pour Windows 2003

Pour démarrer le service Proxy SOL sur un système Windows après l'installation, vous pouvez redémarrer le système (le proxy SOL démarre automatiquement sur un redémarrage). Sinon, vous pouvez démarrer le service Proxy SOL manuellement en effectuant les étapes suivantes :

1. Cliquez-droite sur **Poste de travail** et cliquez sur **Gérer**.

   La fenêtre **Gestion de l'ordinateur** s'affiche.

2. Cliquez sur **Services et applications**, puis sur **Services**.

   Les services disponibles sont affichés sur la droite.

3. Localisez **DSM _BMU_SOLProxy** dans la liste des services et cliquez- droite pour démarrer le service.

En fonction de la console que vous utilisez, il y a différentes étapes pour accéder au serveur proxy SOL. Tout au long de cette section, la station de gestion où le proxy SOL s'exécute est appelée serveur proxy SOL.

Pour Linux

Le serveur proxy SOL démarre automatiquement pendant le démarrage du système. Vous pouvez aussi aller dans le répertoire **/etc/init.d** et utiliser les commandes suivantes pour gérer le service de serveur proxy SOL :

```
solproxy status

dsm_bmu_solproxy32d boot

dsm_bmu_solproxy32d stop

solproxy restart
```

Utilisation de Telnet avec le proxy SOL

Ceci part du principe que le service Proxy SOL est déjà en cours d'exécution sur la station de gestion.

Pour Windows 2003 :

1. Ouvrez une fenêtre d'invite de commande sur votre station de gestion.

2. Saisissez la commande `telnet` dans la ligne de commande et indiquez `localhost` comme adresse IP si le serveur proxy SOL s'exécute sur la même machine et le numéro de port que vous avez spécifié dans l'installation du proxy SOL (la valeur par défaut est 623). Par exemple :

   ```
   telnet localhost 623
   ```

Pour Linux :

1. Ouvrez un environnement Linux sur votre station de gestion.

2. Tapez la commande `telnet` et fournissez `localhost` comme adresse IP du serveur proxy SOL et le numéro de port que vous avez spécifié lors de l'installation du proxy SOL (la valeur par défaut est 623). Par exemple :

   ```
   telnet localhost 623
   ```

REMARQUE : Que votre système d'exploitation hôte soit Windows ou Linux, si le serveur proxy SOL s'exécute sur une machine différente de celle de votre station de gestion, saisissez l'adresse IP du serveur proxy SOL au lieu de localhost.

```
telnet <adresse IP du serveur proxy SOL> 623
```

Utilisation de HyperTerminal avec le proxy SOL

1. Depuis la station distante, ouvrez **HyperTerminal.exe**.

2. Choisissez **TCPIP(Winsock)**.

3. Saisissez l'adresse hôte `localhost` et le numéro de port 623.

Connexion au contrôleur BMC du système géré distant

Lorsqu'une session du proxy SOL a été établie correctement, les choix suivants s'offrent à vous :

```
1. Connect to the Remote Server's BMC (Se connecter au contrôleur BMC du serveur distant)

2. Configure the Serial-Over-LAN for the Remote

Server (Configurer les communications série sur le LAN pour le serveur distant)

3. Activate Console Redirection (Activer la redirection de console)

4. Reboot and Activate Console Redirection (Redémarrer et activer la redirection de console)

5. Help (Aide)

6. Exit (Quitter)
```

REMARQUE : Si plusieurs sessions SOL peuvent être actives en même temps, une seule session de redirection de console peut être active à la fois pour un système géré.

REMARQUE : Pour quitter une session SOL active, utilisez la séquence de caractères <~><.> cette séquence met fin aux communications SOL et vous renvoie au menu supérieur.

1. Sélectionnez l'option 1 du menu principal.

2. Saisissez l'**Adresse IP de l'iDRAC** du système géré distant.

3. Fournissez le **Nom d'utilisateur** et le **Mot de passe** iDRAC6 pour iDRAC6 sur le système géré. Le nom d'utilisateur et le mot de passe iDRAC6 doivent être attribués et stockés dans le stockage rémanent iDRAC6.

   REMARQUE : Une seule session de redirection de console SOL avec iDRAC6 est autorisée à la fois.

   REMARQUE : Si nécessaire, prolongez la durée de la session SOL à l'infini en mettant la valeur **Délai d'attente Telnet** à zéro dans l'interface utilisateur Web iDRAC6 sous **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Services.**

4. Fournissez la clé de cryptage IPMI si elle a été configurée dans l'iDRAC.

   REMARQUE : Vous pouvez localiser la clé de cryptage IPMI dans l'interface utilisateur iDRAC6 dans **Système**→ **Accès à distance**→ **iDRAC**→ **Réseau/Sécurité**→ **Réseau**→ **Paramètres LAN IPMI**→ **Clé de cryptage**.

   REMARQUE : La clé de cryptage IPMI par défaut ne comprend que des zéros. Si vous appuyez sur <Entrée> pour l'option de cryptage, iDRAC6 utilise cette clé de cryptage par défaut.

5. Sélectionnez **Configurer les communications série sur le LAN pour le serveur distant** (option 2) dans le menu principal.

   Le menu de configuration des communications SOL apparaît. En fonction de la condition SOL actuelle, le contenu du menu de configuration des communications SOL varie :

   - Si SOL est déjà activé, les paramètres actuels s'affichent et trois choix vous sont proposés :

     ```
     1. Disable Serial-Over-LAN (Désactiver les communications série sur le LAN)

     2. Change Serial-Over-LAN settings (Modifier les paramètres Communications série sur le LAN)

     3. Cancel (Annuler)
     ```

   - Si SOL est activé, assurez-vous que le débit en bauds SOL est cohérent avec celui d'iDRAC et que le niveau de privilège utilisateur d'**administrateur** minimum iDRAC6 est requis pour activer la redirection de console.
   - Si SOL est actuellement désactivé, tapez `Y` pour activer SOL ou `N` pour laisser SOL désactivé.

- Sélectionnez **Activer la redirection de console** (option 3) dans le menu principal.

  La console texte du système géré distant est redirigée vers votre station de gestion.

7. Sélectionnez **Redémarrer et activer la redirection de console** (option 4) dans le menu principal (en option).

   L'état de l'alimentation du système géré distant est confirmé. S'il est sous tension, vous êtes invité à choisir entre un arrêt normal et un arrêt forcé.

   L'état de l'alimentation est contrôlé jusqu'à ce qu'il soit **activé**. La redirection de console commence et la console texte du système géré distant est redirigée vers votre station de gestion.

   Tandis que le système géré redémarre, vous pouvez accéder au programme de configuration du système BIOS pour afficher ou configurer les paramètres du BIOS.

8. Sélectionnez **Aide** (option 5) dans le menu principal pour afficher une description détaillée pour chaque option.

9. Sélectionnez **Quitter** (option 6) dans le menu principal pour mettre fin à votre session Telnet et vous déconnecter du proxy SOL.

REMARQUE : Si un utilisateur ne termine pas la session SOL correctement, tapez la commande suivante pour redémarrer l'iDRAC. Laissez 1 à 2 minutes à iDRAC6 pour terminer son amorçage. Reportez-vous à la section « Présentation de la sous-commande RACADM » pour plus de détails.

```
racadm racreset
```

Configuration du système d'exploitation

Effectuez les étapes ci-dessous pour configurer les systèmes d'exploitation génériques de type Unix. Cette configuration est basée sur les installations par défaut de Red Hat Enterprise Linux 5.0, de SUSE Linux Enterprise Server 10 SP1 et de Windows 2003 Enterprise.

Système d'exploitation Linux Enterprise

1. Modifiez le fichier **/etc/inittab** pour activer le contrôle du débit matériel et autoriser les utilisateurs à ouvrir une session via la console SOL. Ajoutez la ligne ci-dessous à la fin de la section `#Run gettys in standard runlevels (Exécutez gettys aux niveaux d'exécution standard.)`

```
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
```

Exemple de /etc/inittab original :

```
_____________________________________________________________________

#

# inittab This file describes how the INIT process should set up
# the system in a certain run-level. (Ce fichier décrit comment le
# processus INIT doit configurer) le système sur un certain niveau
# d'exécution.

#


IGNOREZ cette partie du fichier


# Run gettys in standard runlevels (Exécutez gettys aux niveaux d'exécution standard)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1


# Run xdm in runlevel 5 (Exécutez xdm au niveau d'exécution 5)

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

Exemple de /etc/inittab modifié :

```
_____________________________________________________________________

#

# inittab This file describes how the INIT process should set up
# the system in a certain run-level. (Ce fichier décrit comment le processus INIT doit configurer le système sur un certain niveau
d'exécution.)

#


IGNOREZ cette partie du fichier


# Run gettys in standard runlevels (Exécutez gettys aux niveaux d'exécution standard)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1
```

```
3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1

7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Run xdm in runlevel 5 (Exécutez xdm au niveau d'exécution 5)

x:5:respawn:/etc/X11/prefdm -nodaemon
```

---

2. Modifiez le fichier **/etc/securetty** pour permettre aux utilisateurs d'ouvrir une session en tant qu'utilisateur root via la console SOL. Ajoutez la ligne suivante après console :

```
ttyS0
```

Exemple de /etc/securetty original :

```
console

vc/1

vc/2

vc/3

vc/4

IGNOREZ le reste du fichier
```

Exemple de /etc/securetty modifié :

```
Avec la console

ttyS0

vc/1

vc/2

vc/3

vc/4

IGNOREZ le reste du fichier
```

---

3. Modifiez le fichier **/boot/grub/grub.conf** ou **/boot/grub/menu.list** pour ajouter des options de démarrage pour SOL :
   a. Commentez les lignes d'affichage graphique dans les divers systèmes d'exploitation de type Unix :
      - `splashimage=(had0,0)/grub/splash.xpm.gz` dans RHEL 5
      - `gfxmenu (hda0,5)/boot/message` dans SLES 10
   b. Ajoutez la ligne suivante après le premier `title= ...` :

```
# Redirect OS boot via SOL (Redirigez le démarrage du SE via SOL)
```

   c. Ajoutez l'entrée suivante à la première ligne `title= ...` :

```
Redirection SOL
```

   d. Ajoutez le texte suivant à la ligne `kernel/...` du premier `title= ...` :

```
console=tty1 console=ttyS0,115200
```

REMARQUE : **/boot/grub/grub.conf** dans Red Hat Enterprise Linux 5 est un lien symbolique vers **/boot/grub/menu.list**. Vous pouvez modifier les paramètres dans l'un d'eux.

Exemple de /boot/grub/grub.conf d'origine dans RHEL 5 :

```
# grub.conf generated by anaconda (généré par anaconda)

#

# Note that you do not have to return grub after making changes to this (Notez que vous n'avez pas besoin de réexécuter le grub après avoir apporté des modifications à ce)

# file (fichier)

# OTICE: You have a /boot partition. This means that

# all kernel and initrd paths are relative to /boot/,

eg. (AVIS : Vous avez une partition /boot. Cela signifie que tous les chemins du noyau et initrd sont relatifs à /boot/, par exemple)

# root (hd0,0)

# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

# initrd /boot/initrd-version.img

#boot=/dev/sda

default=0

timeout=5

splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu


title Red Hat Enterprise Linux 5

     root (hd0,0)

     kernel /vmlinuz-2.6.18-8,el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet

     initrd /initrd-2.6.18-8,el5,img
```

Exemple de /boot/grub/grub.conf modifié :

```
# grub.conf generated by anaconda (généré par anaconda)

#

# Note that you do not have to return grub after making changes

to this (Notez que vous n'avez pas besoin de réexécuter le grub après avoir apporté des modifications à ce)

# Note that you do not have to return grub after making changes

to this (fichier)

# NOTICE: You have a /boot partition. This means that (AVIS : Vous avez une partition /boot. Cela signifie que)

# all kernel and initrd paths are relative to /boot/,

eg. (tous les chemins du noyau et initrd sont relatifs à /boot/, par exemple)

# root (hd0,0)

# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

# initrd /boot/initrd-version.img

#boot=/dev/sda

default=0

timeout=5
```

```
#splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu


# Redirect the OS boot via SOL (Redirigez le démarrage du SE via SOL)

title Redirection SOL Red Hat Enterprise Linux 5

     root (hd0,0)

     kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet console=tty1 console=ttyS0,115200

     initrd /initrd-2.6.18-8,el5,img
```

Exemple de /boot/grub/menu.list d'origine dans SLES 10 :

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09 (Modifié par YaST2. Dernière modification le sam 11 oct) 21:52:09 UTC 2008

Par défaut 0

Délai d'attente 8

gfxmenu (hd0,5)/boot/message


###Don't change this comment - YaST2 identifier: Original name:

linux (Ne modifiez pas ce commentaire - Identificateur YaST2 : nom d'origine) : linux###

title SUSE Linux Enterprise Server 10 SP1

     root (hd0,5)

     kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

     initrd /boot/initrd-2.6.16.46-0,12-bigsmp
```

Exemple de /boot/grub/menu.list modifié dans SLES 10 :

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09 (Modifié par YaST2. Dernière modification le sam 11 oct 21:52:09) UTC 2008

Par défaut 0

Délai d'attente 8

#gfxmenu (hd0.5)/boot/message


###Don't change this comment - YaST2 identifier: Original name: linux (Ne modifiez pas ce commentaire - Identificateur YaST2 : nom
d'origine : linux)

title SUSE Linux Enterprise Server 10 SP1 SOL redirection

     root (hd0,5)

     kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
     console=tty1 console=ttyS0,115200

     initrd /boot/initrd-2.6.16.46-0,12-bigsmp
```

Windows 2003 Enterprise

1. Déterminez la référence de l'entrée de démarrage en saisissant bootcfg dans l'invite de commande Windows. Localisez la référence de l'entrée de démarrage pour la section comportant le nom convivial du SE **Windows Server 2003 Enterprise**. Appuyez sur <Entrée> pour afficher les options de démarrage sur la station de gestion.

2. Activez EMS à une invite de commande Windows en saisissant :

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <référence de démarrage>
   ```

REMARQUE : <*référence de démarrage*> correspond à la référence de l'entrée de démarrage de l'étape 1.

3. Appuyez sur <Entrée> pour vérifier que le paramètre de la console EMS est effectif.

Exemple de paramètre bootcfg d'origine :

```
_____________________________________________________________________

      Boot Loader Settings

      --------------------

      timeout:30

      default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS


      Boot Entries

      ------------

      Boot entry ID: 1

      Os Friendly Name: Winodws Server 2003, Enterprise

      Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect

_____________________________________________________________________
```

Exemple de paramètre bootcfg modifié :

```
_____________________________________________________________________

      Boot Loader Settings

      --------------------

      timeout: 30

      default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      redirect: COM1

      redirectbaudrate:115200


      Boot Entries

      ------------

      Boot entry ID: 1

      Os Friendly Name: Windows Server 2003, Enterprise

      Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect

_____________________________________________________________________
```

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de la redirection de console de la GUI

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Cette section fournit des informations sur l'utilisation de la fonctionnalité de redirection de console iDRAC6.

Présentation

La fonctionnalité de redirection de console iDRAC6 vous permet d'accéder à distance aux consoles locales en mode graphique ou texte et ainsi de contrôler un ou plusieurs systèmes activés iDRAC6 depuis un emplacement unique.

Utilisation de la redirection de console

REMARQUE : Quand vous ouvrez une session de console, le serveur géré n'indique pas que la console a été redirigée.

L'écran **Redirection de console** vous permet de gérer le système distant en utilisant le clavier, la vidéo et la souris de votre station de gestion locale pour contrôler les périphériques correspondants sur un serveur géré distant. Cette fonctionnalité peut être utilisée conjointement avec la fonctionnalité Média virtuel pour effectuer des installations de logiciels à distance.

Les règles suivantes s'appliquent à une session 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 passante réseau disponible minimale de 1 Mo/s est exigée.

Si un deuxième utilisateur demande une session de redirection de console, le premier utilisateur en est averti et a la possibilité de refuser l'accès, d'autoriser uniquement la vidéo ou d'autoriser un accès partagé complet. Le deuxième utilisateur est averti qu'un autre utilisateur contrôle la session. Le premier utilisateur doit répondre dans les trente secondes ou l'accès complet sera automatiquement accordé au deuxième utilisateur. Pendant toute la durée où deux sessions sont actives simultanément, chaque utilisateur voit un message affiché en haut à droite de l'écran qui identifie l'autre utilisateur ayant une session active. Il n'est pas permis d'ouvrir une troisième session active. Si un troisième utilisateur demande une session de redirection de console, l'accès lui est refusé sans que cela n'interrompe la session du premier ou du second utilisateur.

Si ni le premier ni le deuxième utilisateur ne possèdent de privilèges d'administrateur, la fin de la session active du premier utilisateur entraîne automatiquement la fin de la session du deuxième utilisateur.

Résolutions d'écran prises en charge et taux de rafraîchissement

Tableau 10-1 énumère les résolutions d'écran prises en charge et les taux de rafraîchissement correspondants pour une session de redirection de console qui est exécutée sur le serveur géré.

Tableau 10-1. Résolutions d'écran prises en charge et taux de rafraîchissement

Résolution d'écran	Taux de rafraîchissement (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Configuration de la station de gestion

Pour utiliser la redirection de console sur la station de gestion, procédez comme suit :

1. Installez et configurez un navigateur Web pris en charge. Voir « Navigateurs Web pris en charge » et « 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. Dell vous recommande de configurer la résolution d'affichage de votre moniteur sur 1280 x 1024 pixels.

REMARQUE : 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 l'iKVM pour faire basculer Linux en console textuelle.

Configuration de la redirection de console et du média virtuel dans l'interface Web iDRAC6

Pour configurer la redirection de console dans l'interface Web iDRAC6, effectuez les étapes suivantes :

1. Cliquez sur **Système**, puis sur l'onglet **Console**.
2. Cliquez sur **Configuration** pour ouvrir l'écran **Configuration de la redirection de console**.
3. Configurez les propriétés de la redirection de console. Tableau 10-2 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 10-3.

Tableau 10-2. 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 de clavier et de 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 du 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 **Pas d'accès** si votre serveur ne fonctionne pas sous un système d'exploitation Windows ou Linux. **REMARQUE :** Vous devez sélectionner **Pas d'accès en mode Souris** dans HyperV, Dell Diagnostics ou USC. 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 : *visualiseur de redirection de console Java.* **REMARQUE :** Selon votre version d'Internet Explorer, vous devrez peut-être désactiver des restrictions de sécurité supplémentaires (consultez la section « Configuration et utilisation du média virtuel »). **REMARQUE :** L'environnement d'exécution Java doit être installé sur votre système client pour pouvoir utiliser le visualiseur Java.
Vidéo locale du serveur activée	**Coché** indique que la sortie vers le moniteur iKVM est activée lors de la redirection de console. Décoché indique que les tâches que vous effectuez avec la redirection de console ne sont pas visibles sur le moniteur local du serveur géré.

REMARQUE : Pour obtenir des informations sur l'utilisation du média virtuel avec la redirection de console, consultez la section « Configuration et utilisation du média virtuel ».

Les boutons répertoriés dans Tableau 10-5 sont disponibles sur l'écran **Configuration de la redirection de console**.

Tableau 10-3. Boutons de l'écran Configuration de la redirection de console

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

Ouverture d'une session de redirection de console

Quand vous ouvrez une session de redirection de console, l'application du visualiseur KVM virtuel de Dell démarre et le bureau du système distant apparaît dans le visualiseur. Grâce à l'application 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. Dans l'écran **Redirection de console**, utilisez les informations dans Tableau 10-4 pour garantir qu'une session de redirection de console est disponible.

   Pour reconfigurer les valeurs des propriétés affichées, consultez la section « Configuration de la redirection de console et du média virtuel dans l'interface Web iDRAC6 ».

Tableau 10-4. Informations de l'écran 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 actives.
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 iDRAC6 avec Internet Explorer pendant une exécution sous un système d'exploitation Windows, vous pouvez choisir Active-X ou Java comme type de plug-in.
Vidéo locale du serveur activée	Coché indique que la sortie vers le moniteur iKVM est activée lors de la redirection de console. Décoché garantit que les tâches que vous effectuez avec la **redirection de console** ne sont pas visibles sur le moniteur local du serveur géré.

REMARQUE : Pour obtenir des informations sur l'utilisation du média virtuel avec la redirection de console, consultez la section « Configuration et utilisation du média virtuel ».

Les boutons répertoriés dans Tableau 10-5 sont disponibles sur l'écran **Redirection de console**.

Tableau 10-5. Boutons de l'écran Redirection de console

Bouton	Définition
Actualiser	Recharge l'écran **Configuration de la redirection de console**.
Lancer le visualiseur	Ouvre une session de redirection de console sur le système distant cible.
Imprimer	Imprime l'écran **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 message peuvent apparaître après le lancement de l'application. Afin d'empêcher l'accès non autorisé à l'application, vous devez naviguer à travers ces boîtes de message pendant trois minutes maximum. Sinon, vous serez invité à relancer l'application.

REMARQUE : Si une ou plusieurs fenêtres **Alerte de sécurité** apparaissent au cours des étapes suivantes, lisez les informations qu'elles contiennent et cliquez sur **Oui** pour continuer.

La station de gestion se connecte à iDRAC6 et le bureau du système distant apparaît dans l'application du 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 curseurs de souris».

Utilisation du visualiseur vidéo

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

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.

Tableau 10-6 décrit les options de menu disponibles dans le visualiseur.

Tableau 10-6. 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**.
Keyboard (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 saisissez 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.
Mouse (Souris)	Synchroniser le curseur	Synchronise le curseur afin que la souris sur le client soit redirigée vers la souris sur le serveur.
	Masquer le curseur local	Seul le curseur du KVM s'affiche. Dell recommande d'utiliser ce paramètre lorsque l'USC est exécuté dans un vKVM.
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, consultez la section « Configuration et utilisation du média virtuel ». La fenêtre Visualiseur de console doit rester active lorsque vous utilisez le média virtuel.
Aide	N/A	Active le menu **Aide**.

Synchronisation des curseurs 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 Enterprise Linux ou Novell SUSE Linux, veillez à configurer le mode Souris pour Linux avant de lancer le visualiseur. Consultez la section « Configuration de la redirection de console et du média virtuel dans l'interface Web iDRAC6 » pour obtenir de l'aide sur 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** iDRAC6.

Désactivation ou activation de la console locale

Vous pouvez configurer iDRAC6 pour interdire les connexions iKVM à l'aide de l'interface Web iDRAC6. 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 iDRAC6. 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 dans **l'écran 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 sur iDRAC6. Pour plus d'informations, voir «Accès à l'interface Web».
2. Cliquez sur **Système**, cliquez sur l'onglet **Console**, puis sur **Configuration**.
3. Si vous souhaitez désactiver (mettre sur Arrêt) la vidéo locale sur le serveur, dans l'écran **Configuration de la redirection de console**, décochez la case **Vidéo locale du serveur activée** puis cliquez sur **Appliquer**. La valeur par défaut est **Activé (coché)**.
4. Si vous souhaitez activer (mettre sur Marche) la vidéo locale sur le serveur, dans l'écran **Configuration de la redirection de console**, cochez la case **Vidéo locale du serveur activée** puis cliquez sur **Appliquer**.

L'écran **Redirection de console** affiche la condition de la vidéo locale du serveur.

Questions les plus fréquentes

Tableau 10-7 répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 10-7. 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	Ceci permet à l'utilisateur local d'agir avant que la vidéo ne soit désactivée.

désactiver ?	
Est-ce qu'il y a un délai quand la vidéo locale est activée ?	Non, une fois que la requête d'**activation** de la vidéo locale est reçue par iDRAC6, 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 désactive-t-elle la vidéo sur la session de la console distante ?	Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de la console distante.
Quels sont les privilèges nécessaires à un utilisateur iDRAC6 pour activer ou désactiver la vidéo locale du serveur ?	Tout utilisateur disposant de privilèges de configuration iDRAC6 peut activer ou désactiver la console locale.
Comment connaître l'état actuel de la vidéo locale du serveur ?	La condition est affichée dans l'écran **Configuration de la redirection de console** de l'interface Web iDRAC6. La commande CLI RACADM **racadm getconfig -g cfgRacTuning** affiche la condition dans l'objet **cfgRacTuneLocalServerVideo**. 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 iDRAC6.
Je n'arrive pas à voir le bas de l'écran système à partir de la fenêtre Redirection de console.	Assurez-vous que la résolution du moniteur de la station de gestion est définie sur 1280x1024.
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. Pour de plus amples informations, consultez la section « Configuration des paramètres régionaux sous Linux ».
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 ne se synchronise pas sous DOS pendant la redirection de console. Pourquoi ?	Le BIOS de Dell émule le pilote de souris comme s'il s'agissait d'une souris PS/2. La souris PS/2 est conçue pour utiliser la position relative de son pointeur, ce qui produit un délai de synchronisation. iDRAC6 a un pilote de souris USB, ce qui permet un positionnement absolu et un suivi plus proche du pointeur de la souris. Même si iDRAC6 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 **Pas d'accès** dans la configuration de la redirection de console.
Pourquoi la souris ne se synchronise-t-elle pas dans la console de texte Linux ?	Le KVM virtuel requiert un pilote de souris USB, mais le pilote de souris USB est disponible uniquement sous le système d'exploitation X-Windows.
J'ai toujours des problèmes avec la synchronisation de la souris.	Assurez-vous que la souris appropriée est sélectionnée pour votre système d'exploitation avant de démarrer une session de redirection de console. 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 iDRAC6. Pourquoi ?	Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système dont la fonction de redirection de console est activée dans le BIOS, vous recevez un message de connexion EMS qui vous demande de sélectionner **OK** pour pouvoir continuer. Vous ne pouvez pas utiliser la souris pour sélectionner **OK** à distance. Vous devez sélectionner **OK** sur le système local ou redémarrer le serveur géré à distance, réinstaller puis désactiver la redirection de console dans le BIOS. Ce message est généré par Microsoft pour avertir l'utilisateur que la redirection de console est activée. Pour que ce message n'apparaisse pas, désactivez toujours la redirection de console dans le BIOS avant d'installer un système d'exploitation à distance.
Pourquoi l'indicateur Verr Num sur ma station de gestion ne reflète-t-il pas l'état Verr Num sur le serveur distant ?	Lorsqu'on y accède via iDRAC6, l'indicateur Verr Num sur la station de gestion ne correspond pas nécessairement à l'état du verrouillage numérique sur le serveur distant. L'état Verr Num dépend du paramètre sur le serveur distant lorsqu'une session à distance est ouverte et ne tient pas compte de l'état Verr Num sur la station de gestion.
Pourquoi plusieurs fenêtres Session Viewer apparaissent-elles lorsque j'établis une session de redirection de console à partir de l'hôte local ?	Vous configurez une session de redirection de console à partir du système local. Cette opération n'est pas prise en charge.
Si j'exécute une session de redirection de console et qu'un utilisateur local accède au serveur géré, est-ce que je reçois un message d'avertissement ?	Non Si un utilisateur local accède au système, vous contrôlez tous deux le système.
Quelle est la bande passante nécessaire pour exécuter une session de redirection de console ?	Dell recommande une connexion de 5 Mo/s pour une performance optimale. Une connexion de 1 Mo/s suffit pour une performance minimale.
Quelle est la configuration système minimale requise pour que ma station de gestion exécute la redirection de console ?	La station de gestion nécessite un processeur Intel Pentium III 500 MHz avec au moins 256 Mo de mémoire RAM.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration d'une carte de support VFlash pour utilisation avec iDRAC6

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

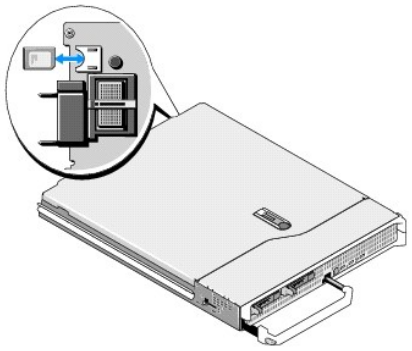
La carte de support VFlash est une carte Secure Digital (SD) qui se connecte dans un logement de carte iDRAC6 Enterprise en option à l'arrière du système. Son espace de stockage se comporte comme toute clé de mémoire flash USB.

Installation d'une carte de support VFlash

REMARQUE : Un support vFlash de marque Dell est requis pour la partition du disque flash virtuel.

1. Retirez le serveur lame du châssis.
2. Localisez le logement de la carte de support VFlash à l'arrière du système.

   REMARQUE : Il n'est pas nécessaire de retirer le capot du serveur lame pour installer ou dégager la carte.



3. Positionnez la carte étiquette orientée vers le haut. Insérez les broches de contact de la carte SD dans le logement correspondant sur le module.

   REMARQUE : Le logement est muni d'un détrompeur qui permet de s'assurer que la carte sera insérée dans le bon sens.

4. Appuyez sur la carte pour qu'elle s'enclenche dans son logement.
5. Replacez le serveur lame dans le châssis.

Retrait d'une carte de support VFlash

Appuyez sur la carte pour la dégager et tirez-la.

Configuration de la carte de support VFlash à l'aide de l'interface Web iDRAC6

Activation ou désactivation de la carte de support VFlash

REMARQUE : La case à cocher **VFlash Enable** (Activer VFlash) est disponible uniquement lorsqu'une carte VFlash est présente. Si le système n'est pas équipé d'une carte, le message suivant s'affiche :

```
SD Card not inserted. Please insert an SD card of size greater than 256MB. (Pas de carte SD insérée. Insérez une carte SD d'une capacité supérieure à 256 Mo.)
```

1. Assurez-vous que la carte VFlash a été installée.

2. Ouvrez une fenêtre d'un navigateur Web pris en charge.
3. Connectez-vous à l'interface Web iDRAC6.
4. Dans l'arborescence Système, cliquez sur **Système**.
5. Cliquez sur l'onglet **VFlash**.

   L'écran **VFlash** apparaît.
6. Cochez la case **Activer VFlash** pour activer la carte de support VFlash. Pour désactiver la carte, désélectionnez la case à cocher.
7. Cliquez sur **Appliquer**.

Formatage de la carte de support VFlash

REMARQUE : L'option **Formater** est disponible uniquement lorsqu'une carte VFlash est présente.

1. Connectez-vous à l'interface Web iDRAC6.
2. Dans l'arborescence Système, cliquez sur **Système**.
3. Cliquez sur l'onglet **VFlash**.

   L'écran **VFlash** apparaît.
4. Assurez-vous que la carte VFlash est désactivée. La case à cocher **VFlash Enable** (Activer VFlash) doit être vide (sans coche).
5. Cliquez sur **Formater**.

   Un message d'alerte indiquant que toutes les images présentes sur la carte sont supprimées lors du formatage s'affiche et vous demande de confirmer l'opération. Cliquez sur **OK** pour continuer.

   Une barre d'état s'affiche, indiquant la progression du formatage.

Téléchargement d'une image de disque

1. Assurez-vous que le fichier image possède l'extension .img et que la taille de l'image est inférieure à 256 Mo.

REMARQUE : Bien que la carte VFlash puisse être supérieure à 256 Mo, seulement 256 Mo sont accessibles à l'heure actuelle.

2. Connectez-vous à l'interface Web iDRAC6.
3. Dans l'arborescence Système, cliquez sur **Système**.
4. Cliquez sur l'onglet **VFlash**.

   L'écran **VFlash** apparaît.
5. Assurez-vous que la carte VFlash est désactivée. La case à cocher **VFlash Enable** (Activer VFlash) doit être vide (sans coche).
6. Dans la section **VFlash Drive** (Lecteur VFlash), tapez le chemin d'accès au fichier image ou cliquez sur **Parcourir** pour accéder à son emplacement sur le système.

   Cliquez sur **Télécharger**.

   Une barre d'état s'affiche, indiquant la progression du téléchargement.

Affichage de la taille de la clé VFlash

Le menu déroulant **Virtual Flash Key Size** (Taille de la clé Flash virtuelle) affiche le paramètre de taille actuel.

Configuration de la carte de support VFlash à l'aide de RACADM

Activation ou désactivation de la carte de support VFlash

Ouvrez une console locale sur le serveur, ouvrez une session et tapez :

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 ou 0 ]
```

où `1` signifie activé, et `0` signifie désactivé.

REMARQUE : Pour plus d'informations sur la commande cfgRacVirtual, y compris le détail des résultats renvoyés, voir la section cfgRacVirtual.

Formatage de la carte de support VFlash

Ouvrez une console texte Telnet/SSH sur le serveur, ouvrez une session et tapez :

```
racadm vmkey reset
```

PRÉCAUTION : Le formatage de la carte de support VFlash supprime toutes les données existantes.

REMARQUE : Pour plus d'informations sur la commande vmkey, voir la section vmkey.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration et utilisation du média virtuel

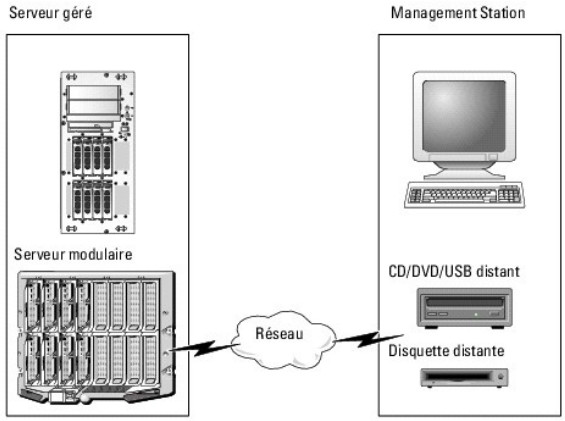
Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

---

Présentation

La fonctionnalité **Média virtuel**, accessible via le visualiseur de redirection de console, permet au serveur géré d'accéder au média connecté à un système distant sur le réseau. Figure 12-1 illustre l'architecture globale d'un **média virtuel**.

Figure 12-1. 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.

Tableau 12-1 énumère les connexions de lecteur prises en charge pour les lecteurs de disquette virtuels et les lecteurs optiques virtuels.

REMARQUE : Le changement de **média virtuel** en cours de connexion est susceptible d'interrompre la séquence de démarrage du système.

Tableau 12-1. Connexions de lecteur prises en charge

Connexions de lecteur de disquette virtuel prises en charge	Connexions de lecteur optique virtuel prises en charge
Lecteur de disquette 1.44 patrimonial avec disquette 1.44	CD-ROM, DVD, CD-RW, lecteur mixte avec média de CD-ROM
Lecteur de disquette USB avec une disquette 1.44	Fichier image de CD-ROM/DVD au format ISO9660
Image de lecteur de disquette 1.44	Lecteur de CD-ROM USB avec média CD-ROM.
Disque USB amovible (taille minimale 128 Mo)	

Station de gestion Windows

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

Selon votre version d'Internet Explorer, vous devrez peut-être définir un paramètre de sécurité personnalisé pour ActiveX :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils**→ **Options Internet**, puis sur l'onglet **Sécurité**.
3. Sous **Sélectionnez une zone de contenu Web pour spécifier ses paramètres de sécurité**, cliquez pour sélectionner la zone souhaitée.
4. Sous **Niveau de sécurité pour cette zone**, cliquez sur **Personnaliser le niveau**.

   La fenêtre **Paramètres de sécurité** s'affiche.
5. Sous **Contrôles ActiveX et plugins**, vérifiez que les paramètres suivants sont définis sur **Activer** :
   - Autoriser les scriptlets
   - Demander confirmation pour les contrôles ActiveX
   - Télécharger les contrôles ActiveX signés
   - Télécharger les contrôles ActiveX non signés
6. Cliquez sur **OK** pour enregistrer les modifications et fermez la fenêtre **Paramètres de sécurité**.
7. Cliquez sur **OK** pour fermer la fenêtre **Options Internet**.
8. Redémarrez Internet Explorer.

Vous devez disposer de droits d'administrateur pour installer ActiveX. Avant d'installer le contrôle ActiveX, Internet Explorer peut afficher un avertissement de sécurité. Pour terminer la procédure d'installation du contrôle ActiveX, acceptez le contrôle ActiveX lorsqu'Internet Explorer affiche un avertissement de sécurité.

Station de gestion Linux

Pour exécuter la fonctionnalité de média virtuel sur une station de gestion exécutant le système d'exploitation Linux, installez une version prise en charge de Firefox. Pour plus d'informations, voir «Navigateurs Web pris en charge».

Un environnement d'exécution Java (JRE) est requis pour exécuter le plug-in de redirection de console. Vous pouvez télécharger une version JRE à l'adresse **java.sun.com**. La version JRE 1.6 ou supérieure est recommandée.

Configuration du média virtuel

1. Connectez-vous à l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Console/Média**.
3. Cliquez sur **Configuration, puis sur Média virtuel**.

   L'écran **Configuration de la redirection de console** s'affiche.
4. Cliquez sur **Média virtuel**.
5. Dans la section **Média virtuel**, sélectionnez des valeurs de paramètres. Voir la section Tableau 12-2 pour plus d'informations sur les valeurs de configuration de **Média virtuel**.
6. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

   Le message d'alerte suivant s'affiche : `You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue?` (Vous êtes sur le point de modifier la configuration du périphérique. Toutes les sessions de redirection seront fermées. Voulez-vous continuer ?)
7. Cliquez sur **OK** pour continuer.

   Le message d'alerte suivant s'affiche : `Virtual Media Configuration successfully set.` (Configuration du média virtuel terminée.)

Tableau 12-2. Valeurs de configuration du média virtuel

Attribut	Valeur
Connecter le média	**Connecter** : connecte immédiatement le **média virtuel** au serveur.

virtuel	**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**. **REMARQUE :** Une seule session utilisateur du média virtuel est autorisée, mais plusieurs périphériques peuvent être connectés au cours d'une même session. Voir « Exécution du média virtuel ».
Sessions actives	Affiche le nombre actuel de sessions de média virtuel.
Cryptage de média virtuel activé	Active (coché) ou désactive (non coché) le cryptage sur les connexions de **média virtuel**.
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 iDRAC6. 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 iDRAC6. 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	Active (coché) ou désactive (non coché) l'option de démarrage une seule fois qui termine automatiquement la session du **média virtuel** après le premier démarrage du serveur. Cette option est utile pour les déploiements automatisés.

Exécution du média virtuel

PRÉCAUTION : N'émettez pas une commande racreset lorsque vous exécutez une session de média virtuel. Sinon, des résultats indésirables peuvent se produire, y compris une perte de données.

REMARQUE : La fenêtre Visualiseur de console doit rester active lorsque vous accédez au média virtuel.

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion.
2. Connectez-vous à l'interface Web iDRAC6.
3. Cliquez sur l'onglet **Console/Média**.

   L'écran de **redirection de console et de média virtuel** s'affiche.

   Si vous souhaitez modifier les valeurs des attributs affichés, voir Configuration du média virtuel.

   REMARQUE : L'option **Fichier image de disquette** dans **Lecteur de disquette** (si applicable) peut apparaître, comme ce périphérique peut être virtualisé comme un lecteur de disquette virtuel. Vous pouvez sélectionner un seul lecteur optique et un seul lecteur de disquette en même temps, ou un seul lecteur.

   REMARQUE : Les lettres du lecteur de périphérique virtuel sur le 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 avancée 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. Sélectionnez **Média** → **Assistant Média virtuel...**

   L'**Assistant Redirection de média** apparaît.

6. Affichez la fenêtre **Condition** au bas de l'écran de l'**assistant**. Si le média est connecté, vous devez le déconnecter avant d'établir une connexion avec une source de média différente. Pour déconnecter un média, cliquez sur le bouton **Déconnecter** situé en regard du média dans la fenêtre **Condition**.
7. Sélectionnez le bouton radio situé en regard des types de média que vous souhaitez connecter.

   Vous pouvez sélectionner le bouton radio **Image disquette** 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 d'accès à l'image sur votre ordinateur local 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 **Fermer.**

Déconnexion du média virtuel

1. Sélectionnez **Média** → **Assistant Média virtuel...**

   L'**Assistant Redirection de média** apparaît.

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 **Close** (Fermer).

Démarrage à partir d'un média virtuel

Le BIOS système vous permet de démarrer à partir de lecteurs optiques virtuels ou de lecteurs de disquette virtuels. Pendant le POST, accédez à la fenêtre Configuration du BIOS et vérifiez que les lecteurs virtuels sont activés et énumérés dans le bon ordre.

Pour changer le paramètre du BIOS, effectuez les étapes suivantes :

1. Démarrez le serveur géré.

2. Appuyez sur<F2> pour entrer dans la fenêtre Configuration du BIOS.

3. Faites défiler jusqu'à la séquence de démarrage et appuyez sur <Entrée>.

   Dans la fenêtre contextuelle, les lecteurs optiques virtuels et les lecteurs de disquette virtuels sont répertoriés avec les périphériques de démarrage standard.

4. Assurez-vous que le lecteur virtuel est activé et énuméré comme étant le premier périphérique avec un média de démarrage. Si nécessaire, suivez les instructions affichées à l'écran pour modifier l'ordre de démarrage.

5. Enregistrez les modifications et quittez.

   Le serveur géré redémarre.

   Le serveur géré essaie de démarrer à partir d'un périphérique d'amorçage en suivant la séquence d'amorçage. Si le périphérique virtuel est connecté et qu'un média de démarrage est présent, le système démarre sur ce périphérique virtuel. Autrement, le système ignore le périphérique, tout comme un périphérique physique sans média de démarrage.

Installation de systèmes d'exploitation avec un média virtuel

Cette section décrit une méthode manuelle interactive pour installer le système d'exploitation sur votre station de gestion, ce qui peut prendre plusieurs heures. Une procédure d'installation sous forme de script du système d'exploitation utilisant le **média virtuel** peut prendre moins de 15 minutes. Pour plus d'informations, voir « Déploiement du système d'exploitation ».

1. Vérifiez les points suivants :
   - Le DVD/CD d'installation de votre système d'exploitation est inséré dans le lecteur de DVD/CD de la station de gestion.
   - Le lecteur de DVD/CD local est sélectionné.
   - Vous êtes connecté aux lecteurs virtuels.

2. Suivez les étapes de démarrage à partir du média virtuel de la section Démarrage à partir d'un média virtuel afin de garantir que le BIOS est configuré pour démarrer à partir du lecteur de DVD/CD à partir duquel vous effectuez l'installation.

3. Suivez les instructions à l'écran pour terminer l'installation.

Utilisation d'un média virtuel pendant l'exécution du système d'exploitation du serveur

Systèmes Windows

Sur les systèmes Windows, les lecteurs de média virtuel sont montés automatiquement s'ils sont connectés et configurés avec une lettre de lecteur.

L'utilisation de lecteurs virtuels à partir de Windows est semblable à l'utilisation de vos lecteurs physiques. Lorsque vous vous connectez au média via l'Assistant Média virtuel, le média est disponible sur le système en cliquant sur le lecteur et en parcourant son contenu.

Systèmes Linux

Selon la configuration du logiciel installé sur votre système, les lecteurs de média virtuel ne peuvent pas être montés automatiquement. Si vos lecteurs ne sont pas montés automatiquement, montez-les manuellement à l'aide de la commande **mount** Linux.

Questions les plus fréquentes

Tableau 12-3 répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 12-3. Utilisation d'un média virtuel : Questions les plus fréquentes

Question	Réponse
Je remarque parfois que ma connexion de client au Média virtuel est interrompue. Pourquoi ?	Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. Si les paramètres de configuration du média virtuel sont modifiés dans l'interface Web iDRAC6 ou via les commandes RACADM locales, tout média connecté est déconnecté lorsque les modifications de la configuration sont appliquées. Pour rétablir la connexion au lecteur virtuel, utilisez l'assistant Média virtuel.
Quels sont les systèmes d'exploitation pris en charge par iDRAC6 ?	Voir Systèmes d'exploitation pris en charge pour obtenir la liste des systèmes d'exploitation pris en charge.
Quels sont les navigateurs Web pris en charge par iDRAC6 ?	Pour une liste des navigateurs Web pris en charge, voir « Navigateurs Web pris en charge ».
Pourquoi m'arrive-t-il parfois de perdre ma connexion client ?	• Vous pouvez parfois perdre votre connexion client si le réseau est lent ou si vous changez le CD dans le lecteur de CD du système client. Par exemple, si vous changez le CD dans le lecteur de CD du système client, le nouveau CD peut avoir une fonctionnalité d'autodémarrage. Si c'est le cas, le micrologiciel peut arriver au bout du délai d'attente, et la connexion peut être perdue si le système client prend trop longtemps avant d'être prêt pour lire le CD. Si une connexion est perdue, reconnectez-vous à partir de la GUI et continuez l'opération précédente. • Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. En outre, il se peut que quelqu'un ait modifié les paramètres de configuration du média virtuel dans l'interface Web ou en ayant entré des commandes RADACM. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité du **média virtuel**.
Une installation du système d'exploitation Windows 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 iDRAC6 en raison de la latence du réseau. Même si la fenêtre d'installation n'indique pas la progression de l'installation, la procédure d'installation est en cours.
Je visualise le contenu d'un lecteur de disquette ou d'une clé mémoire USB. Si j'essaie d'établir une connexion au média virtuel en utilisant le même lecteur, je reçois un message d'échec de connexion et on me demande de réessayer. Pourquoi ?	L'accès simultané aux lecteurs de disquette virtuels n'est pas autorisé. Fermez l'application utilisée pour visualiser le contenu du lecteur avant d'essayer de virtualiser le lecteur.
Comment puis-je configurer mon périphérique virtuel comme périphérique de démarrage ?	Sur le 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 lecteur dans la séquence de démarrage.
À partir de quels types de média puis-je démarrer ?	iDRAC6 vous permet de démarrer à partir des médias de démarrage suivants : • Média de données CD-ROM/DVD • Image ISO 9660 • Disquette 1.44 ou image de disquette • Clé USB qui est reconnue par le système d'exploitation comme disque amovible (taille minimale 128 Mo) • Image de clé USB
Comment faire pour faire de ma clé USB une clé de démarrage ?	Recherchez l'utilitaire de démarrage Dell sur le site **support.dell.com**, un programme Windows que vous pouvez utiliser pour rendre votre clé USB Dell amorçable. Vous pouvez également démarrer à l'aide d'une disquette d'amorçage Windows 98 et copier les fichiers système de la disquette d'amorçage sur votre clé USB. Par exemple, à l'invite du DOS, tapez la commande suivante : `sys a: x: /s` où *x*: est la clé USB que vous voulez utiliser comme clé de démarrage. Vous pouvez également utiliser l'utilitaire de démarrage de Dell pour créer une clé USB de démarrage. Cet utilitaire n'est compatible qu'avec les clés USB de Dell. Pour télécharger l'utilitaire, 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 distante. Que dois-je faire ?	Certaines versions de Linux ne montent pas automatiquement le lecteur de disquette virtuel et le lecteur de CD virtuel de la même manière. Pour installer le lecteur de disquette virtuel, recherchez le nud de périphérique que Linux attribue au lecteur de disquette virtuel. Procédez aux étapes suivantes pour rechercher et monter correctement le lecteur de disquette virtuel : 1. Ouvrez une invite de commande Linux et exécutez la commande suivante : grep "Virtual Floppy" /var/log/messages 2. Recherchez la dernière entrée de ce message et notez l'heure. 3. À l'invite de Linux, exécutez la commande suivante : grep "*hh:mm:ss*" /var/log/messages où *hh:mm:ss* correspond au cachet horaire du message retourné par grep à l'étape 1. 4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique qui est donné à 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 iDRAC6, mes lecteurs virtuels présents sur le serveur ont été supprimés. Pourquoi ?	Les mises à jour du micrologiciel entraînent une réinitialisation d'iDRAC6, une interruption de la connexion à distance et le démontage des lecteurs virtuels. Les lecteurs réapparaîtront une fois la réinitialisation d'iDRAC6 terminée.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de l'interface de ligne de commande RACADM locale

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

L'interface de ligne de commande (CLI) RACADM locale permet d'accéder aux fonctionnalités de gestion iDRAC6 à partir du serveur géré. RACADM permet d'accéder aux mêmes fonctionnalités que l'interface Web iDRAC6. 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 iDRAC6 à partir du serveur géré. Cela signifie que vous pouvez utiliser les commandes RACADM locales pour configurer la mise en réseau iDRAC6 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 iDRAC6 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 d'environnement.

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 iDRAC6.

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

Tableau 13-1 fournit une description de chaque sous-commande RACADM que vous pouvez exécuter dans la RACADM. Pour obtenir une liste détaillée des sous-commandes RACADM, y compris la syntaxe et les entrées valides, voir Présentation de la sous-commande RACADM.

Tableau 13-1. Sous-commandes RACADM

Commande	Description
clrasrscreen	Efface l'écran de la dernière panne.
clrraclog	Efface le journal iDRAC6. 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 iDRAC6.
getconfig	Affiche les propriétés de configuration iDRAC6 actuelles.
getniccfg	Affiche la configuration IP actuelle du contrôleur.
getraclog	Affiche le journal iDRAC6.
getractime	Affiche l'heure iDRAC6.
getssninfo	Affiche des informations sur les sessions actives.
getsvctag	Affiche les numéros de service.
getsysinfo	Affiche des informations sur iDRAC6 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 d'iDRAC6. Si elle est utilisée avec -i, la commande affiche le nombre d'entrées du journal de suivi d'iDRAC6.
help	Répertorie les sous-commandes iDRAC6.
help <*sous-commande*>	Répertorie les instructions d'utilisation pour la sous-commande spécifiée.
localconredirdisable	Effectue la désactivation du kVM local à partir du système local.
racreset	Réinitialise iDRAC6.
racresetcfg	Restaure la configuration par défaut iDRAC6.
serveraction	Effectue des opérations de gestion de l'alimentation sur le serveur géré.
setniccfg	Définit la configuration IP du contrôleur.
sslcertdownload	Télécharge un certificat de CA.
sslcertupload	Télécharge un certificat d'autorité de certification ou un certificat de serveur sur iDRAC6.
sslcertview	Affiche un certificat d'autorité de certification ou un certificat de serveur iDRAC6.
sslcsrgen	Génère et télécharge la CSR SSL.
testemail	Force iDRAC6 à envoyer un e-mail en passant par le NIC iDRAC6.
testtrap	Force iDRAC6 à envoyer une alerte SNMP en passant par le NIC iDRAC6.
vmkey	Restaure la taille par défaut (256 Mo) de la clé de média virtuel.

Utilisation de l'utilitaire RACADM pour configurer iDRAC6

Cette section décrit comment utiliser RACADM pour effectuer diverses tâches de configuration iDRAC6.

Affichage des paramètres iDRAC6 actuels

La sous-commande **getconfig** RACADM récupère les paramètres de configuration actuels à partir d'iDRAC6. 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 iDRAC6 Enterprise pour obtenir une description complète des groupes et des objets.

Pour afficher la liste de tous les groupes iDRAC6, entrez la commande suivante :

```
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 iDRAC6 avec RACADM

REMARQUE : 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 iDRAC6 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 iDRAC6.

REMARQUE : Les utilisateurs et les groupes créés pour les environnements Active Directory doivent se conformer à la convention d'attribution de nom d'Active Directory.

Vous pouvez configurer jusqu'à 15 utilisateurs dans la base de données de propriétés iDRAC6. (Un seizième utilisateur est réservé pour l'utilisateur du LAN IPMI.) Avant d'activer manuellement un utilisateur iDRAC6, vérifiez si des utilisateurs existent déjà.

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 iDRAC6.

Plusieurs paramètres et ID d'objets sont affichés avec leurs valeurs actuelles. Les deux objets d'intérêt 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.

REMARQUE : Les utilisateurs et les groupes créés pour les environnements Active Directory doivent se conformer à la convention d'attribution de nom d'Active Directory.

Ajout d'un utilisateur iDRAC6

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 iDRAC6.
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 iDRAC6 :

```
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 iDRAC6 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 Tableau 13-2 :

Tableau 13-2. Masques binaires pour les privilèges utilisateur

Privilège utilisateur	Masque binaire de privilège
Ouvrir une session iDRAC6	0x0000001
Configurer iDRAC6	0x0000002
Configurer les utilisateurs	0x0000004
Effacer les journaux	0x0000008
Exécuter les commandes de contrôle du serveur	0x0000010
Accéder à la redirection de console	0x0000020
Accéder au média virtuel	0x0000040
Tester les alertes	0x0000080
Exécuter les commandes de débogage	0x0000100

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 iDRAC6

Lorsque vous utilisez la RACADM, les utilisateurs doivent être désactivés manuellement et individuellement. Les utilisateurs ne peuvent pas être supprimés à l'aide d'un fichier de configuration.

L'exemple suivant illustre la syntaxe de commande qui peut être utilisée pour supprimer un utilisateur RAC :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index> ""
```

Une chaîne nulle de guillemets ("") donne l'ordre à iDRAC6 de supprimer la configuration utilisateur à l'index indiqué et de restaurer les valeurs d'usine par défaut de la configuration utilisateur.

Test des alertes par e-mail

La fonctionnalité des alertes par e-mail iDRAC6 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'iDRAC6 peut correctement envoyer des alertes par e-mail sur le réseau.

```
racadm testemail -i 2
```

REMARQUE : Assurez-vous que les paramètres des alertes SMTP et par e-mail sont configurés avant de tester la fonctionnalité d'alertes par e-mail. Pour plus d'informations, voir « Configuration des alertes par e-mail ».

Test de la fonctionnalité d'alertes par interruption SNMP iDRAC6

La fonctionnalité d'alertes par interruption SNMP iDRAC6 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'alerte par interruption SNMP d'iDRAC6, assurez-vous que les paramètres SNMP et d'interruption sont configurés correctement. Voir les descriptions des sous-commandes **testtrap** et **testemail** pour configurer ces paramètres.

Configuration des propriétés du réseau iDRAC6

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

```
racadm getconfig -g cfgLanNetworking
```

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

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

Les commandes fournissent la même fonctionnalité de configuration que l'utilitaire de configuration iDRAC6 lorsque vous êtes invité à taper <Ctrl><E>. Pour plus d'informations sur la configuration des propriétés du réseau à l'aide de l'utilitaire de configuration iDRAC6, voir LAN iDRAC6.

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

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

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

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

Configuration IPMI sur LAN

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 LAN. Pour plus d'informations, consultez 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 définir le privilège du canal LAN IPMI sur 2 (utilisateur), tapez la commande suivante :

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. Définissez la clé de cryptage du canal LAN IPMI, si besoin, à l'aide d'une commande similaire à la suivante :

REMARQUE : L'interface IPMI iDRAC6 prend en charge le protocole RMCP+. Pour plus d'informations, consultez 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 d'IPMI SOL détermine le privilège minimum requis pour activer l'IPMI SOL. Pour plus d'informations, consultez la spécification d'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 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'ID unique de l'utilisateur.

Configuration de PEF

Vous pouvez configurer l'action qu'iDRAC6 devra effectuer pour chaque alerte sur plateforme. Tableau 13-3 répertorie les actions possibles et la valeur permettant de les identifier dans RACADM.

Tableau 13-3. Action d'événement sur plate-forme

Action	Valeur
Pas d'action	0
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 (Tableau 5-7) et <*valeur d'action*> est une valeur de Tableau 13-3.

   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 du 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 le 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 Nom de communauté.

   À l'invite de commande, entrez :

   `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 plate-forme.

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 (plage IP)

Le filtrage des adresses IP (ou *contrôle de plage IP*) permet uniquement un accès à iDRAC6 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 **cfgRacTuning** suivantes :

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propriété **cfgRacTuneIpRangeMask** est appliquée à la fois 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 iDRAC6. Les ouvertures de session à partir d'adresses IP situées à l'extérieur de cette plage reçoivent un message d'erreur.

L'ouverture de session a lieu si l'expression suivante est égale à zéro :

```
cfgRacTuneIpRangeMask & (<adresse IP entrante> ^ cfgRacTuneIpRangeAddr)
```

où & est l'opérateur bitwise AND des quantités et ^ est l'opérateur bitwise exclusif OR.

Voir cfgRacTuning pour une liste complète des propriétés **cfgRacTune**.

Tableau 13-4. 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 accepté 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 des bits de fort poids 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. Dans l'écran **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 : Consultez « Utilisation de l'interface de ligne de commande RACADM locale » pour plus d'informations sur la 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 tout, sauf les deux bits inférieurs dans le masque, comme illustré ci-dessous :

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

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 252.255.255.255
   ```

   Le dernier octet du masque de plage est défini sur 252, l'équivalent décimal de 11111100b.

Instructions concernant le filtrage IP

Observez les instructions suivantes lorsque vous activez le filtrage IP :

- Assurez-vous que **cfgRacTuneIpRangeMask** est configuré sous forme de masque de réseau, où les bits de plus fort poids sont des 1 (ce qui définit le sous-réseau dans le masque) avec une transition de tous les 0 dans les bits de niveau inférieur.
- Utilisez l'adresse de base de la plage de votre choix comme valeur 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 iDRAC6 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 ouvre une session avec succès, l'historique des échecs est effacé et le compteur interne est remis à zéro.

REMARQUE : Lorsque des tentatives d'ouverture de session sont refusées à partir de l'adresse IP client, certains clients SSH peuvent afficher le message suivant : identification: ssh exchange identification: Connection closed by remote host. (Identification d'échange ssh : connexion fermée par l'hôte distant).

Voir « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 Enterprise » pour une liste complète des propriétés **cfgRacTune**.

Propriétés de restriction des nouvelles tentatives d'ouverture de session (blocage IP) répertorie les paramètres définis par l'utilisateur.

Tableau 13-5. Propriétés de restriction des nouvelles tentatives d'ouverture de session (blocage IP)

Propriété	Définition
cfgRacTuneIpBlkEnable	Active la fonctionnalité de blocage IP. Lorsque des échecs consécutifs (**cfgRacTuneIpBlkFailCount**) à partir d'une seule adresse IP sont rencontrés pendant une période de temps spécifique (**cfgRacTuneIpBlkFailWindow**), tous les essais ultérieurs d'établissement d'une session à partir de cette adresse sont rejetés pour un certain temps (**cfgRacTuneIpBlkPenaltyTime)**.
cfgRacTuneIpBlkFailCount	Définit le nombre d'échecs d'ouverture de session à partir d'une adresse IP avant que les tentatives d'ouverture de session ne soient rejetées.
cfgRacTuneIpBlkFailWindow	Le laps de temps, en secondes, au cours duquel les tentatives ayant échoué sont comptées. Lorsque le nombre d'échecs dépasse cette limite, les échecs sont déduits du compte.
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 iDRAC6 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'iDRAC6** pour exécuter les commandes dans cette section.

REMARQUE : Lorsque vous reconfigurez les paramètres Telnet ou SSH dans iDRAC6, 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 commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Pour obtenir la liste complète des commandes de CLI RACADM disponibles, voir Utilisation de l'interface de ligne de commande RACADM locale.

Utilisation d'un fichier de configuration iDRAC6

Un fichier de configuration iDRAC6 est un fichier texte contenant une représentation des valeurs dans la base de données iDRAC6. Vous pouvez utiliser la sous-commande **getconfig** RACADM pour générer un fichier de configuration contenant les valeurs actuelles d'iDRAC6. Vous pouvez ensuite modifier le fichier et utiliser la sous-commande **config -f** RACADM pour recharger le fichier dans iDRAC6 ou pour copier la configuration sur d'autres iDRAC.

Création d'un fichier de configuration iDRAC6

Le fichier de configuration est un fichier texte ordinaire. Vous pouvez utiliser tout 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'iDRAC6 avec la sous-commande **getconfig** RACADM
- Obtenu auprès d'iDRAC6 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

REMARQUE : 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 iDRAC6.

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 (Il s'agit d'un commentaire)

  [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. Ce nom de groupe *doit* être spécifié avant n'importe quel objet dans ce groupe. Les objets auxquels aucun nom de groupe n'est associé génèrent une erreur. Les données de configuration sont organisées en groupes, comme défini dans Définitions des groupes et des objets de la base de données des propriétés iDRAC6 Enterprise.

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

  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.

  L'utilisateur *ne peut pas* spécifier quel index est utilisé. Si l'index existe déjà, il est utilisé ou la nouvelle entrée est créée dans le premier index disponible pour ce groupe.

  La commande `racadm getconfig -f <nom de fichier>` 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 en utilisant la commande suivante :
`racadm config -g <nom de 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.

  L'utilisateur doit supprimer un objet indexé manuellement en utilisant 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 iDRAC6 de supprimer l'index du groupe spécifié.

  Pour voir 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 indexés actuels :

  ```
  [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 d'iDRAC6 de ce groupe. Les objets présents dans ce groupe sont de simples modifications lorsque iDRAC6 est configuré. Si un objet modifié représente un nouvel index, l'index est créé sur iDRAC6 pendant la configuration.

- Vous ne pouvez pas spécifier d'index désiré dans un fichier de configuration.

  Les index peuvent être créés et supprimés, ainsi le groupe peut devenir fragmenté avec des index utilisés et non utilisés. Si un index est présent, il est modifié. Si un index n'est pas présent, le premier index disponible est utilisé. Cette méthode permet une certaine flexibilité lors de l'ajout d'entrées indexées lorsque vous n'avez pas besoin de faire des correspondances d'index exactes entre tous les RAC gérés. De nouveaux utilisateurs sont ajoutés au premier index disponible. Un fichier de configuration qui analyse et s'exécute correctement sur un iDRAC6 peut ne pas s'exécuter correctement sur un autre si tous les index sont remplis et qu'un nouvel utilisateur doit être ajouté.

Modification de l'adresse IP iDRAC6 dans un fichier de configuration

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

Par exemple :

```
#

# Object Group (Groupe d'objet) « cfgLanNetworking »

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#

# (Object Group) Groupe d'objet « cfgLanNetworking »

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (commentaire, le reste de cette ligne est ignoré)

cfgNicGateway=10.35.9.1
```

Chargement du fichier de configuration dans iDRAC6

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 iDRAC6 avec le contenu du fichier.

REMARQUE : Pour vérifier la syntaxe uniquement et ne pas mettre à jour la base de données iDRAC6, 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 iDRAC6.

REMARQUE : Utilisez la sous-commande **racresetcfg** pour réinitialiser la base de données et les paramètres de carte d'interface réseau iDRAC6 et supprimer tous les utilisateurs et les configurations utilisateur. Pendant que l'utilisateur root est disponible, les paramètres par défaut des autres utilisateurs sont également rétablis.

Avant d'exécuter la commande `racadm config -f <nom de fichier>`, vous pouvez exécuter la sous-commande `racresetcfg` pour rétablir les paramètres par défaut de l'iDRAC6. 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 iDRAC6 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 iDRAC6 :

1. Créez le fichier de configuration de l'iDRAC6 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 iDRAC6, comme par exemple **myconfig.cfg**.

   Pour plus d'informations, voir «Création d'un fichier de configuration iDRAC6».

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

4. Pour chaque iDRAC6 que vous souhaitez configurer :

   a. Connectez-vous au serveur géré et démarrez une invite de commande.

   b. Si vous souhaitez reconfigurer iDRAC6 à partir des paramètres par défaut, entrez la commande suivante :

      ```
      racadm racreset
      ```

   c. Chargez le fichier de configuration dans iDRAC6 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'iDRAC6 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 d'iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

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 iDRAC6.

REMARQUE : Cette section suppose que vous connaissez l'initiative SMASH (Systems Management Architecture for Server Hardware) et les spécifications SMWG SM-CLP. Pour plus d'informations sur ces spécifications, consultez le site Web de DMTF (Distributed Management Task Force) à l'adresse **www.dmtf.org**.

SM-CLP iDRAC6 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'iDRAC6, 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 l'adressage des commandes RACADM et SM-CLP.

System Management avec SM-CLP

L'interface SM-CLP iDRAC6 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 : met sous tension, arrête ou redémarre le système
- Gestion du journal des événements système (SEL) : affiche ou efface les enregistrements du journal SEL
- Gestion de compte utilisateur iDRAC6
- Configuration d'Active Directory
- Configuration du LAN iDRAC6
- 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 iDRAC6

L'interface SM-CLP est hébergée par le micrologiciel iDRAC6 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 iDRAC6.

Fonctionnalités de la 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>]
```

Tableau 14-1 fournit une liste des verbes pris en charge par l'interface de ligne de commande iDRAC6, la syntaxe de chaque commande et une liste des options prises en charge par le verbe.

Tableau 14-1. 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, les verbes et les sous-cibles de la cible. 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, -version, -wait
version	Affiche les attributs de version d'une cible. Syntaxe : version [*options*]	-examine, -help, -output, -version

Tableau 14-2 décrit les options SM-CLP. Certaines options ont des formes abrégées, comme indiqué dans le tableau.

Tableau 14-2. 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 iDRAC6. 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 dans Windows et Linux : `..` fait référence au niveau parent et `.` fait référence au niveau actuel.

Cibles

Tableau 14-3 fournit une liste des cibles disponibles dans l'interface SM-CLP.

Tableau 14-3. 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 jusqu'à /system1/sp1/account16	Seize comptes d'utilisateur iDRAC6 locaux. account1 est le compte racine.
/system1/sp1/enetport1	Adresse MAC du NIC iDRAC6.
/system1/sp1/enetport1/lanendpt1/ ipendpt1	Paramètres IP, de passerelle et de masque réseau iDRAC6.
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	Paramètres du serveur DNS iDRAC6.
/system1/sp1/group1 jusqu'à /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 iDRAC6

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 du journal SEL
- Navigation de la cible MAP
- Affichage des propriétés système
- Configuration de l'adresse IP, du masque de sous-réseau et de l'adresse de passerelle iDRAC6

Pour des informations sur l'utilisation de l'interface SM-CLP iDRAC6, voir Base de données des propriétés SM-CLP iDRAC6.

Gestion de l'alimentation du serveur

Tableau 14-4 fournit des exemples d'utilisation de la SM-CLP pour effectuer des opérations de gestion de l'alimentation sur un serveur géré.

Tableau 14-4. Opérations de gestion de l'alimentation du serveur

Opération	Syntaxe
Connexion à iDRAC6 via l'interface SSH	>ssh 192.168.0.120 >login: root -password
Mettre le serveur hors tension	->stop /system1 system1 has been stopped successfully (system1 a été correctement arrêté)
Mettre le serveur sous tension à partir de l'état hors tension	->start /system1 system1 has been started successfully (system1 a été correctement démarré)
Redémarrer le serveur	->reset /system1 system1 has been reset successfully (system1 a été correctement réinitialisé)

Gestion du journal SEL

Tableau 14-5 fournit des exemples d'utilisation de la SM-CLP pour effectuer des opérations SEL sur le système géré.

Tableau 14-5. Opérations de gestion du journal SEL

Opération	Syntaxe
Affichage du journal SEL	->show /system1/sp1/logs1 Cibles : record1 record2 record3 record4 record5 Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs : cd delete exit help show version
Affichage de l'enregistrement du journal 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 (Tous les enregistrements ont été correctement supprimés)

Navigation de la cible MAP

Tableau 14-6 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 14-6. Opérations de navigation de la cible MAP

Opération	Syntaxe
Naviguer vers la cible système et redémarrez	->cd system1 ->reset **REMARQUE :** La cible par défaut actuelle est **/**.
Naviguer vers la cible SEL et afficher les enregistrements du journal	->cd system1 ->cd 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 iDRAC6

L'utilisation de SM-CLP pour mettre à jour les propriétés du réseau iDRAC6 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** : définir sur **1** pour activer la mise en réseau iDRAC6, sur **0** pour la désactiver
   - **ipaddress** : l'adresse IP
   - **subnetmask** : le masque de sous-réseau
   - **oemdell_usedhcp** : définir 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 iDRAC6, 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.

Tableau 14-7 fournit des exemples de configuration des propriétés iDRAC6 via SM-CLP.

Tableau 14-7. Configuration des propriétés de mise en réseau iDRAC6 avec SM-CLP

Opération	Syntaxe
Accéder à l'emplacement des propriétés du NIC iDRAC6	`->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 iDRAC6 via SM-CLP

Pour mettre à jour le micrologiciel iDRAC6 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 iDRAC6 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.

Retour à la page du sommaire

Retour à la page du sommaire

Déploiement du système d'exploitation via iVMCLI

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

L'utilitaire iVMCLI (interface de ligne de commande de média virtuel) 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. En utilisant iVMCLI et des 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 iVMCLI dans votre réseau d'entreprise.

Avant de commencer

Avant de faire appel à l'utilitaire iVMCLI, assurez-vous que vos systèmes distants cibles et votre réseau d'entreprise répondent aux exigences mentionnées dans les sections suivantes.

Exigences du système distant

- iDRAC6 est configuré dans chaque système distant.

Configuration réseau requise

Un partage réseau doit comprendre les composants suivants :

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

  Le fichier image doit être une image de CD de système d'exploitation ou une image ISO de CD/DVD, avec un format de démarrage standard.

Création d'un fichier image de démarrage

Avant de déployer votre fichier image sur les systèmes distants, assurez-vous qu'un système pris en charge peut être démarré à partir du fichier. Pour tester le fichier image, transférez-le vers un système de test à l'aide de l'interface utilisateur Web iDRAC6, puis redémarrez le système.

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

Création d'un fichier image pour les systèmes Linux

Utilisez l'utilitaire de duplicateur de données (dd) pour créer un fichier image de démarrage pour votre système Linux.

Pour exécuter l'utilitaire, ouvrez une invite de commande et entrez la commande suivante :

```
dd if=<périphérique-d'entrée> de=<fichier-de-sortie>
```

Par exemple :

```
dd if=/dev/sdc0 of=mycd.img
```

Création d'un fichier image pour les systèmes Windows

Lorsque vous choisissez un utilitaire de réplicateur de données pour les fichiers image Windows, sélectionnez un utilitaire qui copie le fichier image et les secteurs de démarrage de CD/DVD.

Préparation au déploiement

Configuration des systèmes distants

1. Créez un partage réseau qui puisse être accessible par la station de gestion.
2. Copiez les fichiers de système d'exploitation sur le partage réseau.
3. Si vous avez un fichier image de déploiement de démarrage préconfiguré pour déployer le système d'exploitation sur les systèmes distants, ignorez cette étape.

   Si vous n'avez pas de fichier image de déploiement de démarrage préconfiguré, créez le fichier. Incluez les programmes et/ou scripts utilisés pour les procédures de déploiement de système d'exploitation.

   Par exemple, pour déployer un système d'exploitation 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.

- Effectuez l'une des procédures suivantes :
  - Intégrez **IPMItool** et l'interface de ligne de commande du média virtuel (iVMCLI) 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 iVMCLI 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** fourni avec l'utilitaire iVMCLI. 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 iDRAC6 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*> correspond au nom d'utilisateur iDRAC6, par exemple **root**
- <*idrac-passwd*> correspond au mot de passe de l'utilisateur iDRAC6, par exemple **calvin**
- <*image iso9660*> est le chemin d'accès à une image ISO9660 du CD ou DVD d'installation du système d'exploitation
- <*chemin*> est le chemin d'accès au périphérique contenant le CD ou DVD d'installation du système d'exploitation

Le script **ivmdeploy** transmet ses options de ligne de commande à l'utilitaire **iVMCLI**. Reportez-vous à la section « Options de ligne de commande » pour obtenir des détails sur ces options. Le script traite l'option **-r** de manière légèrement différente de l'option **iVMCLI -r**. Si l'argument de l'option **-r** est le nom d'un fichier existant, le script lit les adresses IP iDRAC6 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'une instance iDRAC6 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 du média virtuel

L'utilitaire iVMCLI est une interface de ligne de commande programmable qui fournit les fonctionnalités de média virtuel de la station de gestion à iDRAC6.

L'utilitaire iVMCLI fournit les fonctionnalités suivantes :

REMARQUE : Lors de la virtualisation de fichiers image en lecture seule, plusieurs sessions peuvent partager le même média image. Lors de la virtualisation de lecteurs physiques, seule une session peut accéder à un lecteur physique donné à la fois.

- Les périphériques de média amovibles ou les fichiers image qui sont en accord avec les plug-in du média virtuel
- L'arrêt automatique lorsque l'option de démarrage unique du micrologiciel iDRAC6 est activée.
- Les communications sécurisées avec iDRAC6 à l'aide du protocole SSL (Secure Sockets Layer)

Avant d'exécuter l'utilitaire, assurez-vous que vous disposez des privilèges utilisateur de média virtuel pour pouvoir exécuter iDRAC6.

Si votre système d'exploitation prend en charge des privilèges d'administrateur, un privilège spécifique de système d'exploitation ou une appartenance au groupe, les privilèges d'administrateur sont également requis pour exécuter la commande iVMCLI.

L'administrateur du système client contrôle les groupes et les privilèges d'utilisateurs, contrôlant ainsi les utilisateurs habilités à exécuter l'utilitaire.

Pour les systèmes Windows, vous devez disposer des droits d'utilisateur privilégié pour pouvoir exécuter l'utilitaire iVMCLI.

Pour les systèmes Linux, vous pouvez accéder à l'utilitaire iVMCLI sans droits d'administrateur, en utilisant la commande **sudo**. Cette commande offre un moyen centralisé de fournir un accès non-administrateur et d'enregistrer toutes les commandes d'utilisateur. Pour ajouter ou modifier des utilisateurs dans le groupe iVMCLI, l'administrateur utilise la commande **visudo**. Les utilisateurs sans droits d'administrateur peuvent ajouter la commande **sudo** comme préfixe à la ligne de commande iVMCLI (ou au script iVMCLI) afin d'accéder à iDRAC6 dans le système distant et d'exécuter l'utilitaire.

Installation de l'utilitaire iVMCLI

L'utilitaire iVMCLI se trouve sur le *DVD Dell Systems Management Tools and Documentation*, qui est inclus avec votre kit logiciel Dell OpenManage System Management. Pour installer l'utilitaire, insérez le *DVD* dans votre système et suivez les instructions qui s'affichent à l'écran.

Le *DVD Dell Systems Management Tools and Documentation* contient les derniers produits logiciels de gestion de systèmes, notamment les diagnostics, la gestion du stockage, le service d'accès à distance et l'utilitaire RACADM. Ce DVD contient aussi des fichiers lisez-moi, qui fournissent les dernières informations sur les produits logiciels de gestion de systèmes.

De plus, le *DVD Dell Systems Management Tools and Documentation* comprend **ivmdeploy**, un exemple de script qui illustre comment utiliser les utilitaires iVMCLI 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 iVMCLI 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 visant à spécifier l'adresse IP iDRAC6 exige la même syntaxe aussi bien pour RACADM que pour iVMCLI.

Le format d'une commande iVMCLI est le suivant :

```
iVMCLI [paramètre] [options d'environnement de système d'exploitation]
```

La syntaxe de ligne de commande respecte la casse. Pour plus d'informations, voir « Paramètres iVMCLI ».

Si le système distant accepte les commandes et si iDRAC6 autorise la connexion, la commande continue de s'exécuter jusqu'à ce qu'un des événements suivants se produise :

- La connexion iVMCLI est interrompue pour une raison ou pour une autre.
- Le processus est manuellement interrompu à l'aide de la commande de système d'exploitation. Par exemple, dans Windows, vous pouvez utiliser le gestionnaire des tâches pour interrompre le processus.

Paramètres iVMCLI

Adresse IP iDRAC6

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

Ce paramètre fournit l'adresse IP iDRAC6 et le port SSL pour lesquels l'utilitaire doit établir une connexion de média virtuel avec l'iDRAC6 cible. Si vous saisissez une adresse IP ou un nom DDNS non valide, un message d'erreur apparaît et la commande est interrompue.

<adresse IP iDRAC> correspond à une adresse IP unique valide ou au nom DDNS (Dynamic Domain Naming System) iDRAC6 (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 iDRAC6 n'ait été modifié, le port SSL optionnel n'est pas requis.

Nom d'utilisateur iDRAC6

```
-u <nom d'utilisateur iDRAC>
```

Ce paramètre fournit le nom de l'utilisateur iDRAC6 qui exécutera le média virtuel.

Le *<nom d'utilisateur iDRAC>* doit avoir les attributs suivants :

- Nom d'utilisateur valide

- Droit d'utilisateur de média virtuel iDRAC6

Si l'authentification iDRAC6 échoue, un message d'erreur s'affiche et la commande se termine.

Mot de passe d'utilisateur iDRAC6

`-p <mot de passe d'utilisateur iDRAC>`

Ce paramètre fournit le mot de passe de l'utilisateur iDRAC6 spécifié.

Si l'authentification iDRAC6 échoue, un message d'erreur s'affiche et la commande se termine.

Périphérique de disquette/disque ou fichier image

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

où <*nom de périphérique*> est une lettre de lecteur valide (pour les systèmes Windows) ou un nom de fichier de périphérique valide, 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/disque virtuel.

Par exemple, un fichier image est spécifié comme :

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

`-f/tmp/myfloppy.img` (système Linux)

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

Par exemple, un périphérique est spécifié comme :

`-f a:\` (système Windows)

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

Si le périphérique fournit une capacité de protection contre l'écriture, utilisez-la pour garantir que le média virtuel n'écrira pas sur le média.

Omettez ce paramètre de la ligne de commande si vous ne virtualisez pas le lecteur de disquette. Si une valeur non valide est détectée, un message d'erreur s'affiche et la commande est interrompue.

Périphérique de CD/DVD ou fichier image

`-c {<nom de périphérique> | <fichier image>}`

où <*nom de périphérique*> est une lettre de lecteur de CD/DVD valide (systèmes Windows) ou un nom de fichier de périphérique de CD/DVD valide (systèmes Linux) et <*fichier image*> est le nom de fichier et le chemin d'un fichier image ISO-9660 valide.

Ce paramètre spécifie le périphérique ou le fichier qui fournira le média virtuel sur CD/DVD-ROM :

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 lecteur CD/DVD. Si une valeur non valide est détectée, un message d'erreur est répertorié et la commande est interrompue.

Spécifiez au moins un type de média (lecteur de disquette ou de CD/DVD) avec la commande, à moins que seules des options de commutateur ne soient fournies. Le cas échéant, un message d'erreur s'affiche et la commande est interrompue en générant une erreur.

Affichage de la version

`-v`

Ce paramètre est utilisé pour afficher la version de l'utilitaire iVMCLI. Si aucune autre option de non-commutateur n'est fournie, la commande est interrompue sans message d'erreur.

Affichage de l'aide

-h

Ce paramètre permet d'afficher un résumé des paramètres de l'utilitaire iVMCLI. Si aucune autre option de non-commutateur n'est fournie, la commande est interrompue sans erreur.

Affichage manuel

-m

Ce paramètre affiche une « page man » détaillée concernant l'utilitaire iVMCLI, incluant les descriptions de toutes les options possibles.

Données cryptées

-e

Lorsque ce paramètre est inclus dans la ligne de commande, iVMCLI utilise un canal crypté SSL pour transférer des données entre la station de gestion et iDRAC6 dans le système distant. Si ce paramètre n'est pas inclus dans la ligne de commande, le transfert de données n'est pas crypté.

Options d'environnement du système d'exploitation iVMCLI

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

- stderr/stdout redirection : redirige la sortie imprimée de l'utilitaire vers un fichier.

  Par exemple, le caractère plus grand que (>), suivi par un nom de fichier, remplace le fichier indiqué par l'impression de l'utilitaire iVMCLI.

  REMARQUE : L'utilitaire iVMCLI ne lit pas les données issues d'une entrée standard (**stdin**). Par conséquent, la redirection **stdin** n'est pas exigée.

- Exécution en arrière-plan : par défaut, l'utilitaire iVMCLI s'exécute au premier 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.

Cette dernière technique est utile dans les programmes de script, car elle permet au script de s'exécuter après le démarrage d'un nouveau processus pour la commande iVMCLI (sans cela, le script serait bloqué jusqu'à ce que le programme iVMCLI soit terminé). Lorsque plusieurs instances iVMCLI sont démarrées de cette manière et qu'une ou plusieurs instances de commande doivent être arrêtées manuellement, utilisez les outils spécifiques au système d'exploitation pour répertorier et terminer les processus.

Codes de retour iVMCLI

0 = aucune erreur

1 = connexion impossible

2 = erreur de ligne de commande iVMCLI

3 = connexion du micrologiciel du RAC coupée

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

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de l'utilitaire de configuration iDRAC6

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

---

Présentation

L'utilitaire de configuration iDRAC6 est un environnement de configuration de prédémarrage vous permettant d'afficher et de définir les paramètres de la carte iDRAC6 et du serveur géré. Vous pouvez notamment :

- Afficher les numéros de révision du micrologiciel pour iDRAC6 et le micrologiciel de fond de panier principal
- Configurer, activer ou désactiver le réseau local iDRAC6
- Activer ou désactiver IPMI sur le LAN
- Configurer les paramètres LAN
- Activer, désactiver ou annuler les services du système
- De connecter ou de déconnecter les périphériques Virtual Media
- Changer le nom d'utilisateur et le mot de passe d'administration
- Rétablir les paramètres d'usine de la configuration iDRAC6
- D'afficher les messages du journal des événements système (SEL) ou d'effacer les messages du journal

Les tâches que vous pouvez effectuer à l'aide de l'utilitaire de configuration iDRAC6 peuvent également être effectuées via d'autres utilitaires fournis par iDRAC6 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 iDRAC6 lors de la configuration iDRAC6 initiale.

Démarrage de l'utilitaire de configuration iDRAC6

Vous devez utiliser une console iDRAC6 connectée à KVM pour accéder initialement à l'utilitaire de configuration iDRAC6 ou après une réinitialisation des paramètres par défaut d'iDRAC6.

1. Sur le clavier connecté à la console KVM iDRAC6, appuyez sur <Impr. écran> pour afficher le menu **OSCAR (On Screen Configuration and Reporting) KVM?iDRAC6**. 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 vous voyez le message, `Press <Ctrl-E> for Remote Access Setup within 5 sec.....(apppuyez sur <Ctrl- E> pour configurer l'accès à distance dans les 5 sec.....)`, appuyez immédiatement sur <Ctrl><E>. L'utilitaire de configuration iDRAC6 s'affiche.

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.

Les deux premières lignes de l'utilitaire de configuration fournissent des informations sur le micrologiciel iDRAC6 et les révisions de micrologiciel de fond de panier primaires. Les niveaux de révision peuvent être utiles afin de déterminer si une mise à niveau du micrologiciel est nécessaire.

Le micrologiciel iDRAC6 est la partie 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 iDRAC6

Sous les messages de révision du micrologiciel, le reste de l'utilitaire de configuration iDRAC6 se compose d'un menu d'éléments auxquels vous pouvez accéder à l'aide de la flèche vers le haut et 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 la barre d'espace pour choisir une valeur.
- Si un élément n'est pas modifiable, il apparaît en bleu. Certains éléments deviennent modifiables en fonction des autres sélections que vous effectuez.
- La dernière ligne de l'écran affiche des instructions concernant l'élément actuel. Vous pouvez appuyer sur <F1> pour afficher l'aide sur l'élément actuel.
- Lorsque vous avez fini d'utiliser l'utilitaire de configuration iDRAC6, appuyez sur <Échap> pour afficher le menu Quitter, dans lequel vous pouvez choisir d'enregistrer ou d'ignorer vos modifications, ou encore de retourner dans l'utilitaire.

Les sections suivantes décrivent les éléments de menu de l'utilitaire de configuration iDRAC6.

LAN iDRAC6

Utilisez la flèche gauche, la flèche droite et la barre d'espace pour choisir entre **Activé** et **Désactivé**.

Le LAN iDRAC6 est désactivé dans la configuration par défaut. Le LAN doit être activé pour permettre l'utilisation des services iDRAC6, 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.)`

Le message vous informe que, outre les services auxquels vous accédez en vous connectant directement aux ports iDRAC6 HTTP, HTTPS, Telnet ou SSH, le trafic réseau de gestion hors bande, tels que les messages IPMI envoyés à iDRAC6 à partir d'une station de gestion, n'est pas reçu lorsque le LAN est désactivé. L'interface RACADM locale reste disponible et peut être utilisée pour reconfigurer le LAN iDRAC6.

`Appuyez sur n'importe quelle touche pour effacer le message et continuer.`

IPMI sur LAN

Appuyez sur la flèche gauche, la flèche droite et la barre d'espace pour choisir entre **Activé** et **Désactivé**. Lorsque **Désactivé** est sélectionné, iDRAC6 n'accepte pas les messages IPMI en provenance de l'interface LAN.

Si vous sélectionnez **Désactivé**, l'avertissement suivant s'affiche :

`iDRAC Out-of-Band interface will be disabled if IPMI`

`Over LAN is OFF. (L'interface hors bande iDRAC sera désactivée si IPMI sur LAN est désactivé.)`

Appuyez sur n'importe quelle touche pour effacer le message et continuer. Pour obtenir une explication du message, voir "LAN iDRAC6".

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 16-1. 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 zéros.
Source d'adresse IP	Choisissez entre **DHCP** et **Statique**. Lorsque DHCP est sélectionné, les champs **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut** sont obtenus auprès d'un serveur DHCP. Si aucun serveur DHCP n'est trouvé sur le réseau, les champs sont définis sur zéro. Lorsque **Statique** est sélectionné, les éléments **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut** deviennent modifiables**.**
Adresse IP Ethernet	Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP obtenue auprès de DHCP. Si la **source d'adresse IP** est définie sur **Statique**, entrez l'adresse IP que vous souhaitez attribuer à iDRAC. L'adresse par défaut est **192.168.0.120** plus le numéro du logement contenant le serveur.
MAC Address (Adresse Mac)	Il s'agit de l'adresse MAC non modifiable de l'interface réseau iDRAC6.
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 de DHCP	Sélectionnez **Activé** pour récupérer les adresses de serveur DNS auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** pour spécifier les adresses de serveur DNS ci-dessous.
Serveur DNS 1	Si **Serveurs DNS de DHCP** est **désactivé**, entrez l'adresse IP du premier serveur DNS.
Serveur DNS 2	Si **Serveurs DNS de DHCP** est **désactivé**, entrez l'adresse IP du deuxième serveur DNS.
Enregistrez le nom iDRAC	Sélectionnez **Activé** pour enregistrer le nom iDRAC6 auprès du service DNS. Sélectionnez **Désactivé** si vous ne voulez pas que les utilisateurs puissent accéder au nom iDRAC6 dans DNS.
Nom 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 iDRAC6 terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom iDRAC6 doit être un nom d'hôte DNS valide.
Nom de domaine de DHCP	Sélectionnez **Activé** si vous souhaitez obtenir le nom de domaine auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** si vous souhaitez spécifier le nom de domaine.
Nom de domaine	Si **Nom de domaine de DHCP** est **désactivé**, appuyez sur <Entrée> pour modifier le champ de texte **Nom de domaine actuel**. Appuyez sur <Entrée> une fois la modification terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom de domaine doit être un domaine DNS valide, par exemple `monentreprise.com`.

Configuration du média virtuel

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. Accédez à l'utilitaire de configuration du BIOS en appuyant sur <F2> lors du démarrage du serveur. Si le **type d'émulation de lecteur Flash USB** est défini sur **Automatique**, le lecteur Flash apparaît sous forme de lecteur de disquette sur le système.

Disque flash virtuel

Utilisez la flèche gauche et la flèche droite pour sélectionner **Activé** ou **Désactivé**.

- **Activer**/**Désactiver** entraîne la **Déconnexion** et la **Connexion** de tous les périphériques de média virtuel du bus USB.
- **Désactiver** entraîne le retrait et l'indisponibilité du flash virtuel.

REMARQUE : Ce champ est en lecture seule si aucune carteSD de taile supérieure à 256 Mo n'est présente dans le logement de carte AMEA.

REMARQUE : Un support VFlash de marque Dell est nécessaire pour la partition du disque flash virtuel.

Configuration des services du système

Services du système

Utilisez la flèche gauche et la flèche droite pour sélectionner **Activé** ou **Désactivé**. Si activées, certaines fonctionnalités iDRAC6 peuvent être configurées via l'utilitaire Unified Server Configurator (USC). Pour plus d'informations, consultez le *Guide de l'utilisateur d'Unified Server Configurator* sur le site web de support de Dell, à l'adresse **support.dell.com**.

REMARQUE : La modification de cette option entraîne le redémarrage du serveur lorsque vous **Enregistrez** et **Quittez** pour appliquer les nouveaux paramètres.

Annuler les services du système

Utilisez la flèche gauche et la flèche droite pour sélectionner **Oui** ou **Non**.

Lorsque vous sélectionnez **Oui**, toutes les sessions d'Unified Server Configurator se ferment, le serveur redémarre lorsque vous **Enregistrez** et **Quittez** pour appliquer les nouveaux paramètres.

Configuration utilisateur LAN

L'utilisateur LAN est le compte administrateur iDRAC6, 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 16-2. Écran de configuration utilisateur LAN

Élément	Description
Accès au compte	Sélectionnez **Activé** pour activer le compte administrateur. Sélectionnez **Désactivé** pour désactiver le compte administrateur.
Privilèges de compte	Choisissez entre **Administrateur**, **Utilisateur**, **Opérateur** et **Aucun accès**.
Nom d'utilisateur de compte	Appuyez sur <Entrée> pour modifier le nom d'utilisateur et appuyez sur <Échap> lorsque vous avez terminé. Le nom d'utilisateur par défaut est **root**.
Entrer le mot de passe	Tapez le nouveau mot de passe du compte administrateur. Les caractères ne sont pas renvoyés sur l'affichage lorsque vous les tapez.
Confirmer le mot de passe	Retapez le nouveau mot de passe du compte administrateur. Si les caractères que vous avez entrés ne correspondent pas à ceux que vous avez tapés dans le champ **Entrer le mot de passe**, un message s'affiche et vous devez entrer à nouveau le mot de passe.

Rétablir les paramètres par défaut

Utilisez l'élément de menu **Rétablir les paramètres par défaut** pour rétablir les paramètres d'usine de tous les éléments de la configuration iDRAC6. Cette opération peut être requise, par exemple, si vous avez oublié le mot de passe utilisateur d'administration ou si vous souhaitez reconfigurer iDRAC6 à partir des paramètres par défaut.

REMARQUE : Dans la configuration par défaut, la mise en réseau iDRAC6 est désactivée. Vous ne pouvez pas reconfigurer iDRAC6 sur le réseau tant que vous n'avez pas activé le réseau iDRAC6 dans l'utilitaire de configuration iDRAC6.

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. Continuer ?

< NON (Annuler) >

< OUI (Continuer) >)
```

Pour rétablir les paramètres par défaut d'iDRAC6, sélectionnez **OUI**, puis appuyez sur <Entrée>.

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>. Pour naviguer :

- 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 spécifique pour atteindre cet enregistrement.

Appuyez sur <Échap> pour quitter le journal des événements système.

REMARQUE : Vous pouvez uniquement effacer les messages du journal SEL dans l'utilitaire de configuration iDRAC6 ou dans l'interface Web iDRAC6.

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 iDRAC6

Lorsque vous avez fini d'apporter des modifications à la configuration iDRAC6, appuyez sur la touche <Échap> pour afficher le menu Quitter.

Sélectionnez **Enregistrer les modifications et quitter** et appuyez sur <Entrée> pour conserver vos modifications.

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 iDRAC6.

Retour à la page du sommaire

Retour à la page du sommaire

Récupération et dépannage du serveur géré

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Cette section explique comment effectuer les tâches relatives au diagnostic et au dépannage d'un serveur géré distant à l'aide des services iDRAC6. 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 iDRAC6 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 : Beaucoup des réparations doivent être assurées par un technicien de manitenance certifié uniquement. 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 dommage causé par une réparation non autorisée par Dell est exclu de votre garantie. Lisez et respectez les consignes de sécurité fournies avec votre produit.**

Voyants inhérents aux problèmes

Cette section décrit les indications concernant les problèmes susceptibles de se produire sur votre système.

Voyants

Le signalement initial de tout problème sur le système peut se faire via les LED présentes sur le châssis ou les composants 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 micrologiciel Dell CMC* pour obtenir de l'aide concernant l'utilisation de l'écran LCD.

Tableau 17-1 décrit les significations de la LED sur le serveur PowerEdge :

Tableau 17-1. 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	iDRAC6 est intègre.
orange clignotant	iDRAC6 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 17-2. Voyants inhérents aux problèmes

Recherchez :	Action :
Les messages d'avertissement du logiciel de gestion des systèmes.	Consultez la documentation du logiciel de gestion des systèmes.
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 d'alerte sur l'écran de condition du serveur sur l'écran LCD	Voir «Vérification des messages d'erreur dans l'écran de condition du serveur».
Messages dans le journal iDRAC6	Voir «Affichage du journal iDRAC6».

Outils de résolution des problèmes

Cette section décrit les services iDRAC6 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
- Vérification des messages d'erreur dans l'écran de condition du serveur sur l'écran LCD
- Affichage du journal iDRAC6
- 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 iDRAC6, le premier écran qui s'affiche décrit l'intégrité des composants système. Tableau 17-3 décrit la signification des voyants d'intégrité du système.

Tableau 17-3. Voyants d'intégrité du système

voyant	Description

	Une coche verte indique une condition saine (normale).
	Un triangle jaune autour d'un point d'exclamation indique une condition d'avertissement (non critique).
	Un X rouge indique une condition critique (défaillance).
	Une icône représentant un point d'interrogation indique que l'état est inconnu.

Cliquez sur un composant quelconque de l'écran **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 écrans d'informations iDRAC6 et CMC contiennent des informations utiles sur la configuration et la condition actuelles.

Vérification du journal des événements système (SEL)

L'écran **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 l'écran **Journal des événements système**.

   L'écran **Journal des événements système** affiche un voyant d'intégrité système (voir Tableau 17-3), un horodateur et une description de l'événement.
3. Cliquez sur le bouton **Journal des événements système** approprié pour continuer (voir Tableau 17-4).

Tableau 17-4. Boutons de SEL

Bouton	Action
Imprimer	Imprime le **journal SEL dans l'ordre de tri qui apparaît dans la fenêtre.**
Effacer le journal	Efface le **journal SEL**. **REMARQUE :** Le bouton **Effacer le journal** n'apparaît que si vous disposez du droit **Effacer les journaux**.
Enregistrer sous	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer le **journal SEL** dans le répertoire de votre choix. **REMARQUE :** Si vous utilisez Internet Explorer et rencontrez un problème lors de l'enregistrement, téléchargez Cumulative Security Update for Internet Explorer à partir du site Web de support de Microsoft® à l'adresse support.microsoft.com.
Actualiser	Recharge l'écran du **journal SEL**.

Vérification des codes du POST

L'écran **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 système BIOS, 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**.

   L'écran **Codes du POST** affiche un voyant d'intégrité système (voir Tableau 17-3), un code hexadécimal et une description du code.
2. Cliquez sur le bouton approprié de l'écran **Codes du POST** pour continuer (voir Tableau 17-5).

Tableau 17-5. Boutons du code du POST

Bouton	Action
Imprimer	Imprime l'écran **Codes du POST.**
Actualiser	Recharge l'écran **Codes du POST.**

Affichage de l'écran de la dernière panne système

REMARQUE : La fonctionnalité Écran de la dernière panne doit être configurée dans Server Administrator et dans l'interface Web iDRAC6. Voir Configuration du serveur géré pour la saisie de l'écran du dernier plantage pour obtenir des instructions sur la configuration de cette fonctionnalité.

L'**écran de la dernière panne** affiche l'écran de la panne la plus récente, qui comprend des informations sur les événements qui se sont produits avant la panne du système. L'image de la dernière panne du système est enregistrée dans le magasin permanent d'iDRAC6 et est accessible à distance.

Pour afficher l'**écran de la dernière panne**, effectuez les étapes suivantes :

- Cliquez sur **Système**, cliquez sur l'onglet **Journaux**, puis sur **Dernière panne**.

L'**écran de la dernière panne** inclut les boutons présentés dans Tableau 17-6 :

REMARQUE : Les boutons **Enregistrer** et **Supprimer** n'apparaissent pas en l'absence d'écran de panne enregistré.

Tableau 17-6. Boutons de l'écran de la dernière panne

Bouton	Action
Imprimer	Imprime l'**écran de la dernière panne**.
Enregistrer	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer l'**écran de la dernière panne** dans le répertoire de votre choix.
Supprimer	Supprime l'**écran de la dernière panne**.
Actualiser	Recharge l'**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. Le paramètre 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. Pour plus d'informations, voir « Configuration du serveur géré pour la saisie de l'écran du dernier plantage ».

Visualisation des dernières séquences de démarrage

Si vous rencontrez des problèmes lors de l'amorçage, vous pouvez visualiser à l'écran les événements qui se sont produits au cours des trois dernières séquences d'amorçage dans l'écran **Saisie de l'amorçage**. Les écrans d'amorçage sont lus à la vitesse de 1 trame par seconde. Tableau 17-7 énumère les actions de contrôle disponibles.

REMARQUE : Vous devez posséder des privilèges d'administrateur pour lire les séquences de saisie de l'amorçage.

Tableau 17-7. Options de saisie de l'amorçage

Bouton / Option	Description
Sélectionner la séquence d'amorçage	Vous permet de sélectionner la séquence d'amorçage à charger et à lire. - Saisie de l'amorçage 1 : charge la dernière séquence d'amorçage. - Saisie de l'amorçage 2 : charge la (deuxième plus récente) séquence d'amorçage qui s'est produite avant la saisie de l'amorçage 1. - Saisie de l'amorçage 3 : charge la (troisième plus récente) séquence d'amorçage qui s'est produite avant la saisie de l'amorçage 2.
Enregistrer sous	Crée un fichier .zip compressé contenant toutes les images de saisie de l'amorçage de la séquence courante. L'utilisateur doit posséder des privilèges d'administrateur pour effectuer cette action.
Écran précédent	Vous ramène à l'écran précédent, le cas échéant, dans la console de relecture.
Lire	Lance le scénario depuis l'écran actuel dans la console de relecture.
Pause	Met en pause le scénario sur l'écran actuel affiché dans la console de relecture.
Arrêter	Arrête le scénario et charge le premier écran de cette séquence d'amorçage.
Écran suivant	Vous amène à l'écran suivant, le cas échéant, dans la console de relecture.
Imprimer	Imprime l'image de saisie de l'amorçage qui apparaît à l'écran.
Actualiser	Recharge l'écran Saisie de l'amorçage.

Vérification des messages d'erreur dans l'écran de condition du serveur

Lorsqu'une LED orange clignote, et qu'une erreur s'est produite sur un serveur particulier, l'écran de condition du serveur sur l'écran LCD met en surbrillance le serveur affecté en orange. Utilisez les boutons de navigation de l'écran LCD pour mettre en surbrillance le serveur affecté, puis cliquez sur le bouton central. Les messages d'erreur et d'avertissement s'affichent sur la deuxième ligne. Le tableau suivant répertorie tous les messages d'erreur et leur gravité.

Tableau 17-8. Écran Condition du serveur

Severity	Message	Cause
Avertissement	System Board Ambient Temp: Temperature sensor for System Board, warning event (Temp ambiante de la carte système : capteur de température de la carte système, événement d'avertissement.)	La température ambiante du serveur a franchi un seuil d'avertissement.
Critique	System Board Ambient Temp: Temperature sensor for System Board, failure event (Temp. ambiante de la carte système : capteur de température de la carte système, événement de panne)	La température ambiante du serveur a franchi un seuil de panne.
Critique	System Board CMOS Battery: Battery sensor for System Board, failed was asserted (Batterie CMOS de la carte système : capteur de batterie de la carte système, la panne a été confirmée.)	La batterie CMOS est absente ou sa tension est nulle
Avertissement	System Board System Level: Current sensor for System Board, warning event (Niveau système de la carte système : capteur de courant de la carte système, événement d'avertissement)	Le courant a franchi un seuil d'avertissement
Critique	System Board System Level: Current sensor for System Board, failure event (Niveau système de la carte système : capteur de courant de la carte système, événement de panne)	Le courant a franchi un seuil de panne
Critique	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (UC<numéro> <nom du capteur de tension> : capteur de tension de l'UC<numéro>, l'état confirmé a été confirmé)	Tension hors plage
Critique	System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted (Carte système <nom du capteur de tension> : capteur de tension de la carte système, l'état confirmé a été confirmé)	Tension hors plage
Critique	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (UC<numéro> <nom du capteur de tension> : capteur de tension de l'UC<numéro>, l'état confirmé a été confirmé)	Tension hors plage
Critique	CPU<number> Status: Processor sensor for CPU<number, IERR was asserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, l'IERR a été confirmé)	Panne de l'UC
Critique	CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, le dépassement thermique a été confirmé)	UC surchauffée
Critique	CPU<number> Status: Processor sensor for CPU<number, configuration error was asserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, l'erreur de configuration a été confirmée)	Type de processeur incorrect ou dans un emplacement erroné
Critique	CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, la confirmation de la présence a été annulée)	L'UC requise est manquante ou est absente.
Critique	System Board Video Riser: Module sensor for System Board, device removed was asserted (Carte de montage vidéo de la carte système : capteur de module de la carte système, le périphérique retiré a été confirmé)	Le module requis a été retiré
Critique	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted (Condition de la carte Mezz B<numéro de logement> : capteur de carte d'extension de la carte Mezz B<numéro de logement>, l'erreur d'installation a été confirmée)	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted(Condition de la carte Mezz C<numéro de logement> : capteur de carte d'extension de la carte Mezz C<numéro de logement>, l'erreur d'installation a été confirmée)	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed (Lecteur de fond de panier <numéro> : capteur de logement du lecteur de fond de panier, lecteur retiré)	Le lecteur de stockage a été retiré.
Critique	Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted (Lecteur de fond de panier <numéro> : capteur de logement du lecteur de fond de panier, la panne du lecteur a été confirmée)	Le lecteur de stockage a échoué.
Critique	System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted (Prévention de défaillance PFault de la carte système : capteur de tension de la carte système, l'état confirmé a été confirmé)	Cet événement est généré lorsque les tensions de la carte système ne sont pas aux niveaux normaux.
Critique	System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, le délai expiré a été confirmé)	Le registre d'horloge de la surveillance iDRAC6 a expiré et aucune action n'est définie.
Critique	System Board OS Watchdog: Watchdog sensor for System Board, reboot was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, le redémarrage a été confirmé)	La surveillance iDRAC6 a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte), et que l'action est définie sur redémarrage.
Critique	System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, la mise hors tension a été confirmée)	La surveillance iDRAC6 a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte), et que l'action est définie sur mise hors tension.
Critique	System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, le cycle d'alimentation a été confirmé)	La surveillance iDRAC6 a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte), et que l'action est définie sur cycle d'alimentation.
Critique	System Board SEL: Event Log sensor for System Board, log full was asserted (Journal SEL de la carte système : capteur du journal d'événements de la carte système, la plénitude du journal a été confirmée)	Le périphérique du journal SEL détecte qu'une seule entrée peut être ajoutée au journal SEL avant qu'il ne soit plein.
Avertissement	ECC Corr Err: Memory sensor, correctable ECC (<DIMM Location>) was asserted(ECC Corr Err : capteur de mémoire, l'ECC corrigeable (<emplacement de la barrette DIMM>) a été confirmée)	Les erreurs ECC corrigeables ont atteint un taux critique.
Critique	ECC Uncorr Err: Memory sensor, uncorrectable ECC (<DIMM Location>) was asserted (Err ECC non corr : capteur de mémoire, l'ECC non corrigeable (<emplacement de la barrette DIMM>) a été confirmée)	Une erreur ECC non corrigeable a été détectée.
Critique	I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted (Contr du	Une interruption critique est générée dans le canal

	canal d'E/S : capteur d'événement critique, le NMI du contrôle du canal d'E/S a été confirmé)	d'E/S.
Critique	PCI Parity Err: Critical Event sensor, PCI PERR was asserted (Err de parité PCI : capteur d'événement critique, le PERR PCI a été confirmé)	Une erreur de parité a été détectée sur le bus PCI.
Critique	PCI System Err: Critical Event sensor, PCI SERR (<Slot number or PCI Device ID>) was asserted (Erreur du système PCI : capteur d'événement critique, le SERR PCI (<numéro de logement ou réf. périphérique PCI>) a été confirmé.)	Erreur PCI détectée par le périphérique
Critique	SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted (Journal SBE désactivé : capteur du journal d'événements, la journalisation des erreurs mémoire corrigeables a été confirmée)	La journalisation des erreurs portant sur un seul bit est désactivée lorsqu'un nombre trop élevé de SBE est journalisé
Critique	Logging Disabled: Event Log sensor, all event logging disabled was asserted (Journalisation désactivée : capteur du journal d'événements, la journalisation systématique des événements désactivée a été confirmée)	La journalisation de toutes les erreurs est désactivée
Irrécupérable	CPU Protocol Err: Processor sensor, transition to nonrecoverable was asserted (Err protocole de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée.)	Le protocole du processeur est passé à l'état irrécupérable.
Irrécupérable	CPU Bus PERR: Processor sensor, transition to non-recoverable was asserted (PERR du bus de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée.)	Le PERR du bus du processeur est passé à l'état irrécupérable.
Irrécupérable	CPU Init Err: Processor sensor, transition to non-recoverable was asserted (Err d'init de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée.)	L'initialisation du processeur est passée à l'état irrécupérable.
Irrécupérable	CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted (Machine Check de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée)	Le Machine Check du processeur est passé à l'état irrécupérable.
Critique	Memory Spared: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Mémoire de secours : capteur de mémoire, la redondance perdue (<emplacement de la barrette DIMM>) a été confirmée)	La mémoire de secours n'est plus redondante.
Critique	Memory Mirrored: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Mémoire en miroir : capteur de mémoire, la redondance perdue (<emplacement de la barrette DIMM>) a été confirmée)	La mémoire en miroir n'est plus redondante.
Critique	Memory RAID: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Mémoire en miroir : capteur de mémoire, la redondance perdue (<emplacement de la barrette DIMM>) a été confirmée)	La mémoire RAID n'est plus redondante.
Avertissement	Memory Added: Memory sensor, presence (<DIMM Location>) was deasserted (Mémoire ajoutée : capteur de mémoire, la confirmation de la présence (<emplacement de la barrette DIMM>) a été annulée)	Le module de mémoire ajouté a été retiré.
Avertissement	Memory Removed: Memory sensor, presence (<DIMM Location>) was deasserted (Mémoire retirée : capteur de mémoire, la confirmation de la présence (<emplacement de la barrette DIMM>) a été annulée)	Le module de mémoire a été retiré.
Critique	Memory Cfg Err: Memory sensor, configuration error (<DIMM Location>) was asserted (Err config mémoire : capteur de mémoire, l'erreur de configuration (<emplacement de la barrette DIMM>) a été confirmée)	La configuration de la mémoire est incorrecte pour le système.
Avertissement	Mem Redun Gain: Memory sensor, redundancy degraded (<DIMM Location>) was asserted (Gain redon mém : capteur de mémoire, la redondance dégradée (<emplacement de la barrette DIMM>) a été confirmée)	La redondance de la mémoire est rétrogradée, mais n'est pas perdue.
Critique	PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted (Err fatale PCIE : capteur d'événement critique, l'erreur fatale du bus a été confirmée)	Une erreur fatale a été détectée sur le bus PCIE.
Critique	Chipset Err: Critical Event sensor, PCI PERR was asserted (Err jeu de puces : capteur d'événement critique, le PERR PCI a été confirmé)	Une erreur de puce a été détectée.
Avertissement	Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location>) was asserted (Avertissement ECC mém : capteur de mémoire, la transition de OK à non critique (<emplacement de la barrette DIMM>) a été confirmée)	Les erreurs corrigeables de l'ECC ont dépassé le taux normal.
Critique	Mem ECC Warning: Memory sensor, transition to critical from less severe (<DIMM Location>) was asserted (Avertissement ECC mém : capteur de mémoire, la transition de moins grave à critique (<emplacement de la barrette DIMM>) a été confirmée.)	Les erreurs ECC corrigeables ont atteint un taux critique.
Critique	POST Err: POST sensor, No memory installed (Err POST : capteur POST, mémoire non installée)	Mémoire non détectée sur la carte
Critique	POST Err: POST sensor, Memory configuration error (Err POST : capteur POST, erreur de configuration de la mémoire)	Mémoire détectée mais non configurable
Critique	POST Err: POST sensor, Unusable memory error (Err POST : capteur POST, erreur de mémoire inutilisable)	Mémoire configurée mais inutilisable
Critique	POST Err: POST sensor, Shadow BIOS failed (Err POST : capteur POST, le BIOS en double a échoué.)	Panne du BIOS en double système
Critique	POST Err: POST sensor, CMOS failed (Err POST : capteur POST, le CMOS a échoué.)	Panne du CMOS
Critique	POST Err: POST sensor, DMA controller failed (Err POST : capteur POST, le contrôleur DMA a échoué.)	Panne du contrôleur DMA
Critique	POST Err: POST sensor, Interrupt controller failed (Err POST : capteur POST, le contrôleur d'interruptions a échoué)	Panne du contrôleur d'interruptions
Critique	POST Err: POST sensor, Timer refresh failed (Err POST : capteur POST, l'actualisation du temporisateur a échoué.)	Panne d'actualisation du temporisateur
Critique	POST Err: POST sensor, Programmable interval timer error (Err POST : capteur POST, erreur du temporisateur d'intervalle programmable)	Erreur du temporisateur d'intervalle programmable
Critique	POST Err: POST sensor, Parity error (Err POST : capteur POST, erreur de parité)	Erreur de parité
Critique	POST Err: POST sensor, SIO failed (Err POST : capteur POST, le SIO a échoué.)	Panne du SIO
Critique	POST Err: POST sensor, Keyboard controller failed (Err POST : capteur POST, le contrôleur du clavier a échoué)	Défaillance du contrôleur de clavier
Critique	POST Err: POST sensor, System management interrupt initialization failed (Err POST : capteur POST, l'initialisation de System Management Interrupt a échoué.)	Panne d'initialisation de System Management Interrupt
Critique	POST Err: POST sensor, BIOS shutdown test failed (Err POST : capteur POST, le test	Panne du test d'arrêt du BIOS

	d'arrêt du BIOS a échoué.)	
Critique	POST Err: POST sensor, BIOS POST memory test failed (Err POST : capteur POST, le test de mémoire POST du BIOS a échoué.)	Panne du test mémoire du POST du BIOS.
Critique	POST Err: POST sensor, Dell remote access controller configuration failed (Err POST : capteur POST, la configuration du contrôleur Dell Remote Access Controller a échoué.)	Panne de la configuration du contrôleur Dell Remote Access Controller
Critique	POST Err: POST sensor, CPU configuration failed (Err POST : capteur POST, la configuration de l'UC a échoué.)	Panne de configuration de l'UC
Critique	POST Err: POST sensor, Incorrect memory configuration (Err POST : capteur POST, configuration de la mémoire incorrecte)	Configuration de la mémoire incorrecte
Critique	POST Err: POST sensor, POST failure (Err POST : capteur POST, panne du POST)	Panne générale après la vidéo
Critique	Hdwar version err: Version Change sensor, hardware incompatibility was asserted (Err de version de matériel : capteur de modification de matériel, l'incompatibilité du matériel a été confirmée)	Un matériel incompatible a été détecté
Critique	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted (Err de version de matériel : capteur de modification de matériel, l'incompatibilité du matériel (micrologiciel BMC) a été confirmée)	Le matériel est incompatible avec le micrologiciel
Critique	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted (Err de version de matériel : capteur de modification de matériel, l'incompatibilité du matériel (micrologiciel BMC et non-correspondance de l'UC) a été confirmée)	L'UC et le micrologiciel ne sont pas compatibles
Critique	Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted (Surchauffe de mém : capteur de mémoire, l'ECC corrigeable (<emplacement de la barrette DIMM>) a été confirmé)	Le module de mémoire est en surchauffe
Critique	Mem Fatal SB CRC: Memory sensor, uncorrectable ECC was asserted (CRC SB irrécupérable de mém : capteur de mémoire, l'ECC non corrigeable a été confirmé.)	Panne de mémoire Southbridge
Critique	Mem Fatal NB CRC: Memory sensor, uncorrectable ECC was asserted (CRC NB irrécupérable de mém : capteur de mémoire, l'ECC non corrigeable a été confirmé.)	Panne de mémoire Northbridge
Critique	WatchDog Timer: Watchdog sensor, reboot was asserted (Registre d'horloge de la surveillance : capteur de la surveillance, le redémarrage a été confirmé)	Le registre d'horloge de la surveillance a provoqué le redémarrage du système
Critique	WatchDog Timer: Watchdog sensor, timer expired was asserted (Registre d'horloge de la surveillance : capteur de la surveillance, le délai expiré a été confirmé)	Le registre d'horloge de la surveillance a expiré, mais aucune action n'a été prise
Avertissement	Link Tuning: Version Change sensor, successful software or F/W change was deasserted (Réglage de liaison : capteur de changement de version, la confirmation du changement réussi de logiciel ou de micrologiciel a été annulée.)	La mise à jour du paramètre de réglage de liaison pour un fonctionnement NIC correct a échoué.
Avertissement	Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted (Réglage de liaison : capteur de changement de version, la confirmation de la changement réussie du matériel <numéro de logement du périphérique> a été annulée)	La mise à jour du paramètre de réglage de liaison pour un fonctionnement NIC correct a échoué.
Critique	LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Function #) was asserted (Rég liaison/Adr. flex : capteur de réglage de liaison, l'échec de programmation de l'adresse MAC virtuelle (Bus # Périphérique # Fonction #) a été confirmé)	L'adresse flex n'a pas pu être programmée pour ce périphérique
Critique	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) was asserted (Rég liaison/Adr. flex : capteur de réglage de liaison, l'échec de la prise en charge du réglage de liaison ou de l'adresse flex (Mezz <emplacement>) par la mémoire morte en option du périphérique a été confirmé.)	La mémoire morte en option ne prend pas en charge l'adresse flex ou le réglage de liaison.
Critique	LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted (Rég liaison/Adr. flex : capteur de réglage de liaison, l'échec de l'obtention des données de réglage de liaison ou d'adresse flex de BMC/iDRAC6 a été confirmé.)	Échec de l'obtention des informations de réglage de liaison ou d'adresse flex de BMC/iDRAC6
Critique	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz XX) was asserted (Rég liaison/Adr. flex : capteur de réglage de liaison, l'échec de la prise en charge du réglage de liaison ou de l'adresse flex (Mezz <emplacement>) par la mémoire morte en option du périphérique a été confirmé)	Cet événement est généré lorsque la mémoire morte en option du périphérique PCI pour un NIC ne prend pas en charge le réglage de liaison ou la fonctionnalité d'adressage flex.
Critique	LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted(Rég liaison/Adr. flex : capteur de réglage de liaison, l'échec de la programmation de l'adresse MAC virtuelle (<emplacement>) a été confirmé)	Cet événement est généré lorsque le BIOS échoue à programmer l'adresse MAC virtuelle sur le périphérique NIC donné.
Critique	I/O Fatal Err: Fatal IO Group sensor, fatal IO error (<location>) (Err fatale E/S : capteur de groupe d'E/S fatales, erreur d'E/S fatales (<emplacement>))	Cet événement est généré en association avec un IERR de CPU et indique le périphérique qui en est la cause.
Avertissement	PCIE NonFatal Er: Non Fatal I/O Group sensor, PCIe error (<location>) (Er non fatale PCIE : capteur de groupe d'E/S non fatales, erreur PCIe (<emplacement>))	Cet événement est généré en association avec un IERR de CPU.

Affichage du journal iDRAC6

Le **journal iDRAC6** est un journal permanent conservé dans le micrologiciel iDRAC6. Le journal contient une liste des actions d'utilisateur (ouverture, fermeture de sessions et modifications des règles de sécurité, par exemple) et des alertes envoyées par iDRAC6. Les entrées les plus anciennes sont écrasées 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 iDRAC6.

Pour accéder au **journal iDRAC**, effectuez les étapes suivantes :

- Cliquez sur **Système**→ **Accès à distanceÆ** iDRAC, puis cliquez sur **Journal iDRAC**.

Le **journal iDRAC** contient les informations répertoriées dans Tableau 17-9.

Tableau 17-9. Informations du journal iDRAC6

Champ	Description
Date/Heure	Date et heure (par exemple, 19 Déc 16:55:47). iDRAC6 définit son horloge en fonction de l'horloge du serveur géré. Si iDRAC6 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	Interface qui a provoqué l'événement.
Description	Description brève de l'événement et nom d'utilisateur qui s'est connecté à iDRAC6.

Utilisation des boutons du journal iDRAC6

L'écran **Journal iDRAC** dispose des boutons suivants (voir Tableau 17-10) :

Tableau 17-10. Boutons du journal iDRAC6

Bouton	Action
Imprimer	Imprime l'écran **Journal iDRAC**.
Effacer le journal	Efface les entrées du **journal iDRAC**. **REMARQUE :** Le bouton **Effacer le journal** n'apparaît que si vous avez le droit **Effacer les journaux**.
Enregistrer sous	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer le **journal iDRAC** dans le répertoire de votre choix. **REMARQUE :** Si vous utilisez Internet Explorer et rencontrez un problème lors de l'enregistrement, téléchargez Cumulative Security Update for Internet Explorer à partir du site Web de support de Microsoft à l'adresse **support.microsoft.com**.
Actualiser	Recharge l'écran **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

Tableau 17-11 et Tableau 17-12 décrivent les propriétés de l'enceinte principale du système.

Tableau 17-11. Champs Informations 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 de l'hôte	Indique le nom du système hôte.
Nom du système d'exploitation	Indique le système d'exploitation fonctionnant sur le système.

Tableau 17-12. Champs de récupération automatique

Champ	Description
Action de récupération	Lorsqu'un *arrêt imprévu du système* est détecté, iDRAC6 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	Le nombre de secondes écoulées après la détection d'un *arrêt imprévu du système* avant qu'iDRAC6 n'effectue une action de

initial	récupération.
Compte à rebours actuel	Valeur actuelle, en secondes, du compte à rebours.

Integrated Dell Remote Access Controller

Tableau 17-13 décrit les propriétés d'iDRAC6.

Tableau 17-13. Champs d'informations d'iDRAC6

Champ	Description
Date/Heure	Indique la date et l'heure actuelles sur iDRAC6 en GMT.
Version du micrologiciel	Indique la version du micrologiciel iDRAC6.
Mise à jour du micrologiciel	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.
par défaut	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.
MAC Address (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 M1000e contient jusqu'à seize serveurs. Pour rechercher un serveur spécifique dans le châssis, vous pouvez utiliser l'interface Web iDRAC6 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. Dans l'écran **Identifier**, cochez la case **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. Dans l'écran **Identifier**, désélectionnez la case **Identifier le serveur**.
3. Cliquez sur **Appliquer**.

Utilisation de la console de diagnostics

L'iDRAC6 fournit un ensemble standard d'outils de diagnostic réseau (voir Tableau 17-14) qui sont semblables aux outils fournis avec les systèmes Microsoft® Windows® ou Linux. À l'aide de l'interface Web iDRAC6, vous pouvez accéder aux outils de débogage réseau.

Pour accéder à l'écran **Console de diagnostics**, effectuez les étapes suivantes :

1. Cliquez sur **Système**→ **iDRAC**→ **Dépannage**.
2. Cliquez sur l'onglet **Diagnostics**.

Tableau 17-14 décrit les commandes qui peuvent être entrées sur l'écran **Console de diagnostics**. Tapez une commande et cliquez sur **Envoyer**. Les résultats

du débogage apparaissent dans l'écran **Console de diagnostics**.

Cliquez sur le bouton **Effacer** pour effacer les résultats affichés par la commande précédente.

Pour actualiser l'écran **Console de diagnostics**, cliquez sur **Actualiser**.

Tableau 17-14. Commandes de diagnostic

Commande	Description
arp	Affiche le contenu de la table du protocole de résolution d'adresses (ARP). Les entrées ARP ne peuvent être ni ajoutées ni supprimées.
ifconfig	Affiche le contenu de la table d'interface réseau.
netstat	Imprime le contenu de la table de routage.
ping *<adresse IP>*	Vérifie que l'adresse IP de destination est accessible à partir d'iDRAC6 avec le contenu actuel du tableau de routage. Il faut saisir une adresse IP de destination dans le champ à droite de cette option. Un paquet d'écho du protocole de contrôle des messages sur Internet (ICMP) est envoyé à l'adresse IP de destination en fonction du contenu actuel de la table de routage.
gettracelog	Affiche le journal de suivi d'iDRAC6. Pour plus d'informations, voir « gettracelog ».

Gestion de l'alimentation d'un système distant

iDRAC6 vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance sur un serveur géré. Utilisez l'écran **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 **Exécuter les commandes d'action du serveur** pour effectuer les actions de gestion de l'alimentation. Voir Ajout et configuration des utilisateurs iDRAC6 pour obtenir de l'aide sur 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)**.

   Tableau 17-15 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 17-15.

Tableau 17-15. 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. **REMARQUE :** Un arrêt normal du système d'exploitation du serveur n'est parfois pas possible lorsque le logiciel du serveur cesse de répondre ou si aucun administrateur n'a ouvert de session sur la console locale d'un système Windows. Dans ces cas, vous devez demander le redémarrage forcé de Windows au lieu d'un arrêt normal. De plus, selon la version du système d'exploitation Window, une stratégie peut être configurée autour du processus d'arrêt et risque de modifier le comportement de l'arrêt lorsqu'il est déclenché à partir d'iDRAC6. Consultez la documentation de Microsoft pour connaître la règle de l'ordinateur local « Arrêt : autoriser l'arrêt du système sans avoir à ouvrir une session ».
Réinitialiser le système (redémarrage à chaud)	Redémarre le système sans le mettre hors tension (redémarrage à chaud).
Effectuer un cycle d'alimentation système	Met le système hors tension, puis le redémarre (redémarrage à froid).

Tableau 17-16. Boutons de gestion de l'alimentation

Bouton	Action
Imprimer	Imprime les valeurs de **Gestion de l'alimentation** qui apparaissent à l'écran.
Actualiser	Recharge l'écran **Gestion de l'alimentation**.
Appliquer	Enregistre les nouveaux paramètres que vous créez pendant l'affichage de l'écran Gestion de l'alimentation.

Dépannage et questions les plus fréquentes

Tableau 17-17 contient les questions les plus fréquentes sur les problèmes de dépannage.

Tableau 17-17. 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 iDRAC6 : • Voir « Vérification du journal des événements système (SEL) ». À partir de la commande SM-CLP : • Voir « Gestion du journal SEL ». À partir de l'utilitaire de configuration iDRAC6 : • Voir « 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 obtenir des informations sur cette fonction.
Comment puis-je trouver l'adresse IP de iDRAC6 ?	Depuis l'interface Web CMC : 1. Cliquez sur **Châssis**→ **Serveurs**, puis cliquez 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 iDRAC6 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 micrologiciel CMC* pour accéder à la liste complète des sous-commandes RACADM CMC. Vous pouvez également utiliser la commande **getsysinfo** RACADM pur afficher l'adresse IP d'iDRAC6.

	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 iDRAC6 : • Cliquez sur **Système**→ **Accès à distance**→ **CMC**. L'adresse IP CMC s'affiche dans l'écran **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 micrologiciel CMC* 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 iDRAC6 ne fonctionne pas.	• Assurez-vous que le câble LAN est connecté à CMC. • Assurez-vous que le LAN iDRAC6 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.	• iDRAC6 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 iDRAC6.	Vous devez rétablir les paramètres par défaut d'iDRAC6. 1. Redémarrez le serveur et appuyez sur <Ctrl><E> lorsque le système vous y invite afin d'entrer dans l'utilitaire de configuration iDRAC6. 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 iDRAC6, un message contextuel de sécurité ActiveX apparaît.	iDRAC6 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 iDRAC6 à la liste des sites sécurisés : 1. Cliquez sur **Outils**→ **Options Internet...**→ **Sécurité**→ **Sites approuvés**. 2. Cliquez sur **Sites** et entrez l'adresse IP ou le nom DNS d'iDRAC6. 3. Cliquez sur **Add** (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.
iDRAC6 ne démarre pas.	Retirez et réinsérez le serveur. Allez dans l'interface Web CMC afin de déterminer si iDRAC6 apparaît en tant que composant pouvant être mis à niveau. Si tel est le cas, suivez les instructions dans Mise à jour du micrologiciel iDRAC6 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 iDRAC6 à partir de l'interface Web iDRAC6 ou de l'écran LCD.

Retour à la page du sommaire

Retour à la page du sommaire

Glossaire

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise pour serveurs lames Version 2.0 Guide d'utilisation

Active Directory

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

AGP

Abréviation d'Accelerated Graphics Port (port graphique accéléré), une spécification du bus qui permet aux cartes graphiques d'accéder plus rapidement à la mémoire du système principal

ARP

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

ASCII

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

BIOS

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

CMC

Abréviation de Enclosure Management Controller (contrôleur de gestion de l'enceinte), l'interface de contrôleur entre iDRAC6 et le contrôleur CMC du système géré.

bus

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

AC

Une autorité de certification est une entité commerciale reconnue dans l'industrie de l'informatique pour ses critères élevés en matière de dépistage et d'identification fiables et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples de CA. Une fois que la CA a reçu votre CSR, ils examinent et vérifient les informations contenues dans la CSR. Si le demandeur satisfait aux normes de sécurité de l'autorité de certification, celle-ci lui émet un certificat qui identifie le demandeur de manière unique pour les transactions réseau et Internet.

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).

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.

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 volumineux exécuté 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.

DDNS

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

DMTF

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

DNS

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

Carte iDRAC6

Abréviation de Dell Remote Access Controller 6 Enterprise.

DSU

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

schéma étendu

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

FQDN

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

FSMO

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

GMT

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

GPIO

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

GRUB

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

GUI

Abréviation de Graphical User Interface (interface utilisateur graphique), une interface d'affichage informatique qui utilise des éléments tels que 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 saisie sous forme de texte.

journal du matériel ;

Enregistre les événements générés par iDRAC6 et le contrôleur CMC.

iAMT

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

ICMB

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

ICMP

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

ID

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

Carte iDRAC6

Sigle d'Integrated Dell Remote Access Controller 6, le système de contrôle/surveillance « Système sur une puce » intégré des serveurs Dell 10G PowerEdge.

IP

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

IPMB

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

IPMI

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

Kb/s

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

LAN

Abréviation de Local Area Network (réseau local).

LDAP

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

Voyant

Abréviation de Light-Emitting Diode (diode électroluminescente).

LOM

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

MAC

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

adresse MAC

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

serveur géré

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

Station de gestion

La station de gestion est le système qui accède à iDRAC6 à distance.

MAP

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

Mb/s

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

MIB

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

MII

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

NAS

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

Carte réseau (NIC)

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

OID

Abréviation d'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 iDRAC6 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 mis sous tension.

PPP

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

RAM

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

disque RAM

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

RAC

Abréviation de Remote Access Controller.

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.

RSC

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

tr/min

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

Console SAC

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

SAP

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

SEL

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

SMI

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

SMTP

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

SMWG

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

interruption SNMP

Une notification (événement) générée par le contrôleur iDRAC6 ou CMC qui contient des informations sur les changements d'état du serveur géré ou sur des problèmes matériels potentiels.

SSH

Abréviation de Secure Shell (protocole de connexions sécurisées) .

SSL

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

schéma standard

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

TAP

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

TCP/IP

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

TFTP

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

Onduleur

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

USB

Abréviation de Universal Serial Bus (bus série universel).

UTC

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

VLAN

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

VNC

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

VT-100

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

WAN

Abréviation de Wide Area Network (réseau étendu).

Retour à la page du sommaire

Retour à la page du sommaire

Version 2.0 Guide d'utilisation

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

PRÉCAUTION : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données en cas de non-respect des instructions.

Mars 2009 Rév. A00

Retour à la page du sommaire