# Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3



## Remarques et précautions

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

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




Décembre 2009

Retour à la page du sommaire

# Présentation de la sous-commande RACADM

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



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

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

---

## help

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-1. Commande help**

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

## Synopsis

```
racadm help

racadm help <sous-commande>
```

## Description

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

## Sortie

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

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

## arp

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

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

**Tableau A-2. Commande arp**

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

## Synopsis

```
racadm arp
```

## Interfaces prises en charge

- RACADM distante
- RACADM Telnet/ssh/série

---

## clearasrscreen

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

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

**Tableau A-3. clearasrscreen**

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

## Synopsis

```
racadm clearasrscreen
```

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

## config

**REMARQUE :** Pour utiliser la commande **getconfig**, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-4. config/getconfig**

| Sous-commande | Définition |
|---|---|
| **config** | Configure iDRAC6. |
| **getconfig** | Obtient les données de configuration iDRAC6. |

## Synopsis

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

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

## Description

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

**REMARQUE :** Le fichier de configuration récupéré via la racadm distante et la racadm locale n'est pas interopérable. Le fichier de configuration récupéré via la racadm distante affiche la propriété d'index d'une partie des groupes indexés en lecture-écriture, par exemple cfgSSADRoleGroupIndex. Dans la cas de la commande « config -f <nom de fichier> », utilisez le fichier de configuration récupéré depuis la même interface. Par exemple, pour la racadm locale « config -f <nom de fichier> », utilisez le fichier généré à partir de la commande racadm locale « getconfig -f <nom de fichier> ».

### Entrée

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

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

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

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

### Sortie

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

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

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

### Exemples

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

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

- `racadm config -f myrac.cfg`

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

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

  **REMARQUE :** Pour configurer l'action PEF du filtre d'assertion d'informations de la carte SD, vous ne pouvez pas utiliser la commande racadm locale. Utilisez plutôt la commande racadm distante : `racadm -r <adresse ip iDRAC6> -u <nom d'utilisateur> -p <calvin> config -g cfgIpmipef -i 20 -o cfgIpmipefaction [0-3]`.

---

# getconfig

## Description de la sous-commande getconfig

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

### Entrée

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

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

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

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

### Sortie

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

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

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

## Exemples

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig –f myrac.cfg`

  Enregistre tous les objets Configuration de groupe iDRAC6 sur **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 claires sur les valeurs de propriétés.

## Synopsis

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

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

racadm getconfig -u <nom d'utilisateur>

racadm getconfig -h
```

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# coredump

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

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

**Tableau A-7. coredump**

| Sous-commande | Définition |
|---|---|
| **coredump** | Affiche le dernier vidage de mémoire iDRAC6. |

## Synopsis

```
racadm coredump
```

## Description

La sous-commande **coredump** affiche des informations détaillées concernant les problèmes critiques récents qui se sont produits avec le RAC. Les informations coredump peuvent être utilisées pour diagnostiquer ces problèmes critiques.

Si disponibles, les informations coredump sont permanentes sur les cycles d'alimentation iDRAC6 et restent disponibles jusqu'à ce qu'une des conditions suivantes se produise :

- Les informations coredump sont effacées avec la sous-commande **coredumpdelete**.
- Une autre condition critique se produit sur le RAC. Dans ce cas, les informations coredump portent sur la dernière erreur critique qui s'est produite.

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

## Interfaces prises en charge

- RACADM distante
- RACADM Telnet/ssh/série

---

# coredumpdelete

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

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

**Tableau A-8. coredumpdelete**

| Sous-commande | Définition |
|---|---|
| **coredumpdelete** | Supprime le vidage de mémoire stocké sur iDRAC6. |

## Synopsis

```
racadm coredumpdelete
```

## Description

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

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

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# fwupdate

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC6**.

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

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

**Tableau A-9. fwupdate**

| Sous-commande | Définition |
|---|---|
| **fwupdate** | Met à jour le micrologiciel sur iDRAC6. |

## Synopsis

```
racadm fwupdate -s

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

racadm fwupdate -r
```

## Description

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

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série (l'option **-p** n'est pas prise en charge avec la console série/Telnet/ssh)

## Entrée

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

**REMARQUE :** L'option **-p** est prise en charge sur la RACADM locale et distante, et n'est pas prise en charge avec la console série/Telnet/ssh. L'option **-p** n'est pas non plus prise en charge sur les systèmes d'exploitation Linux.

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

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

## Sortie

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

## Exemples

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

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

- `racadm fwupdate -s`

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

**REMARQUE :** La mise à jour de micrologiciel de la RACADM distante via le chemin local n'est pas prise en charge sur les systèmes d'exploitation Linux.

---

# getssninfo

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-11. Sous-commande getssninfo**

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

## Synopsis

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

## Description

La commande **getssninfo** renvoie une liste des utilisateurs connectés à iDRAC6. Les informations récapitulatives fournissent les informations suivantes :

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

## Entrée

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

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

| Option | Description |
|---|---|
| **-A** | L'option **-A** élimine l'impression des en-têtes de données. |
| **-u** | L'option de nom d'utilisateur, **-u <***nom d'utilisateur***>**, limite la sortie imprimée aux enregistrements de session détaillés concernant le nom d'utilisateur donné. Si un symbole « * » est donné en tant que nom d'utilisateur, tous les utilisateurs sont répertoriés. Les informations récapitulatives ne sont pas imprimées lorsque cette option est spécifiée. |

## Exemples

- `racadm getssninfo`

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

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

| Utilisateur | Adresse IP | Type | Consoles |
|---|---|---|---|
| root | 192.168.0.10 | Telnet | KVM virtuel |

- `racadm getssninfo -A`

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

- `racadm getssninfo -A -u *`

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

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

---

## getsysinfo

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-14. 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] [-c] [-4] [-6] [-r]
```

## Description

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

**REMARQUE :** La sous-commande local racadm *getsysinfo* sous Linux affiche la *longueur de préfixe* sur des lignes distinctes pour les adresses IPv6 2 à 15 et pour l'adresse locale du lien.

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

## Entrée

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

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

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

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

## Sortie

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

## Exemple de sortie

```
RAC Information:
```

RAC Date/Time = 10/27/2009 14:38:00

Firmware Version = 1.30

Firmware Build = 20

Last Firmware Update = 10/26/2009 16:55:08

Hardware Version = 0.01

MAC Address = 00:24:e8:2e:c5:d3

Common settings:

Register DNS RAC Name = 1

DNS RAC Name = eval710-08-r

Current DNS Domain = blr.amer.dell.com

Domain Name from DHCP = 1

IPv4 settings:

Enabled = 1

Current IP Address = 10.94.20.134

Current IP Gateway = 10.94.20.1

Current IP Netmask = 255.255.254.0

DHCP Enabled = 1

Current DNS Server 1 = 163.244.180.39

Current DNS Server 2 = 163.244.180.40

DNS Servers from DHCP = 1

IPv6 settings:

Enabled = 1

Current IP Address 1 = ::

Current IP Gateway = ::

Autoconfig = 1

Link Local IP Address = fe80::224:e8ff:fe2e:c5d3/255

Current IP Address 2 = ::

Current IP Address 3 = ::

Current IP Address 4 = ::

Current IP Address 5 = ::

Current IP Address 6 = ::

Current IP Address 7 = ::

Current IP Address 8 = ::

Current IP Address 9 = ::

Current IP Address 10 = ::

Current IP Address 11 = ::

Current IP Address 12 = ::

Current IP Address 13 = ::

Current IP Address 14 = ::

Current IP Address 15 = ::

DNS Servers from DHCPv6 = 0

Current DNS Server 1 = ::

```
Current DNS Server 2 = ::

System Information:

System Model = PowerEdge R710

System BIOS Version = 1.0.4

Service Tag = 2X2Q12S

Host Name = WIN-IHF5D2BF5SN

OS Name =

Power Status = ON

Embedded NIC MAC Addresses:

NIC1 Ethernet = 00:24:e8:2e:c5:cb

iSCSI = 00:24:e8:2e:c5:cc

NIC2 Ethernet = 00:24:e8:2e:c5:cd

iSCSI = 00:24:e8:2e:c5:ce

NIC3 Ethernet = 00:24:e8:2e:c5:cf

iSCSI = 00:24:e8:2e:c5:d0

NIC4 Ethernet = 00:24:e8:2e:c5:d1

iSCSI = 00:24:e8:2e:c5:d2

Watchdog Information:

Recovery Action = None

Present countdown value = 15 seconds

Initial countdown value = 15 seconds
```

## Exemples

- `racadm getsysinfo -A -s`

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

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

- `racadm getsysinfo -w -s`

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


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

## Restrictions

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

---

# getractime

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-16. getractime**

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

## Synopsis

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

## Description

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

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

## Sortie

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

## Exemple de sortie

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# ifconfig

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Exécuter des commandes de diagnostic** ou **Configurer iDRAC**.

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

**Tableau A-17. ifconfig**

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

## Synopsis

```
racadm ifconfig
```

---

# netstat

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

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

**Tableau A-18. netstat**

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

## Synopsis

```
racadm netstat
```

## Interfaces prises en charge

- RACADM distante
- RACADM Telnet/ssh/série

---

# ping

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Exécuter des commandes de diagnostic** ou **Configurer iDRAC**.

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

**Tableau A-19. ping**

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

## Synopsis

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

## Interfaces prises en charge

- RACADM distante
- RACADM Telnet/ssh/série

---

# setniccfg

**REMARQUE :** Pour utiliser la commande **setniccfg**, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-20. setniccfg**

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

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

## Synopsis

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <adresse IPv4> <masque de réseau> <passerelle IPV4>

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

racadm setniccfg -o
```

## Description

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

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

## Sortie

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# getniccfg

**REMARQUE :** Pour utiliser la commande **getniccfg**, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-21. setniccfg/getniccfg**

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

## Synopsis

```
racadm getniccfg
```

## Description

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

## Exemple de sortie

La sous-commande **getniccfg** affiche un message d'erreur approprié si l'opération a échoué. Sinon, en cas de réussite, la sortie est affichée au format

suivant :

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# getsvctag

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-22. getsvctag**

| Sous-commande | Définition |
|---|---|
| **getsvctag** | Affiche un numéro de service. |

## Synopsis

```
racadm getsvctag
```

## Description

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

## Exemple

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

```
Y76TP0G
```

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# racdump

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Déboguer**.

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

**Tableau A-23. racdump**

| Sous-commande | Définition |
|---|---|
| **racdump** | Affiche des informations sur la condition et des informations générales concernant iDRAC6. |

## Synopsis

```
racadm racdump
```

## Description

La sous-commande **racdump** fournit une seule commande pour obtenir les informations sur le vidage et la condition, et des informations générales sur une carte iDRAC6.

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

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

## Interfaces prises en charge

- RACADM distante
- RACADM Telnet/ssh/série

---

# racreset

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-24. 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 [hard | soft]
```

## Description

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

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

**REMARQUE :** Vous devez redémarrer votre système après avoir effectué une réinitialisation matérielle d'iDRAC6 comme décrit dans le tableau A-25.

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

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

| | |
|---|---|

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

## Exemples

- `racadm racreset`

  Démarre la séquence de réinitialisation logicielle d'iDRAC6.

- `racadm racreset hard`

  Démarre la séquence de réinitialisation matérielle d'iDRAC6.

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# racresetcfg

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-26. racresetcfg**

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

## Synopsis

```
racadm racresetcfg
```

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

## Description

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

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

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

---

# serveraction

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

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

**Tableau A-27. serveraction**

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

## Synopsis

```
racadm serveraction <action>
```

## Description

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

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

| Chaîne | Définition |
|---|---|
| ***<action>*** | Spécifie l'action. Les options de la chaîne <*action*> sont :<br>• **powerdown :** met le système géré hors tension.<br>• **powerup :** met le système géré sous tension.<br>• **powercycle :** lance une opération de cycle d'alimentation sur le système géré. Cette action est semblable à une pression sur le bouton d'alimentation situé sur le panneau avant du système pour mettre hors tension, puis sous tension le système.<br>• **powerstatus :** affiche la condition actuelle de l'alimentation du serveur (« ACTIVÉ » ou « DÉSACTIVÉ »)<br>• **hardreset :** effectue une opération de réinitialisation (redémarrage) sur le système géré. |

## Sortie

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# getraclog

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-29. getraclog**

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

## Synopsis

```
racadm getraclog -i

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

## Description

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

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

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

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

## Sortie

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

## Exemple de sortie

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# clrraclog

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

## Synopsis

```
racadm clrraclog
```

## Description

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

---

# getsel

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-30. getsel**

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

## Synopsis

```
racadm getsel -i
```

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

## Description

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

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

**-A :** spécifie la sortie sans affichage d'en-tête ou d'étiquette.

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

**-o :** affiche la sortie sur une seule ligne.

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

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

**-R :** seules les données brutes sont imprimées.

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

**REMARQUE :** Si aucun argument n'est spécifié, le journal est affiché dans son intégralité.

## Sortie

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

Par exemple :

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# clrsel

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

## Synopsis

```
racadm clrsel
```

## Description

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# gettracelog

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Ouvrir une session sur iDRAC**.

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

**Tableau A-31. gettracelog**

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

## Synopsis

```
racadm gettracelog -i

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

## Description

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

**-**i : affiche le nombre d'entrées du journal de suivi d'iDRAC6.

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

**-o :** affiche la sortie sur une seule ligne.

**-c :** spécifie le nombre d'enregistrements à afficher

**-s :** spécifie l'enregistrement de démarrage à afficher

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

## Sortie

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

Par exemple :

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

## sslcsrgen

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-32. sslcsrgen**

| Sous-commande | Description |
|---|---|
| **sslcsrgen** | Génère et télécharge une requête de signature de certificat (RSC) 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 RSC et télécharger le fichier dans le système de fichiers local du client. La RSC peut servir à créer un certificat SSL personnalisé qui peut être utilisé pour les transactions SSL sur le RAC.

## Options

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

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

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

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

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

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

La sous-commande **sslcsrgen -s** renvoie un des codes de condition suivants :

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

## Restrictions

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

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

### Exemples

```
racadm sslcsrgen -s

ou

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série (l'option **-f** n'est pas prise en charge pour la console série/Telnet/ssh)

---

# sslcertupload

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-34. sslcertupload**

| Sous-commande | Description |
|---|---|
| **sslcertupload** | Téléverse un serveur SSL personnalisé ou un certificat d'une AC pour le service de répertoire à partir du client vers le RAC. |

## Synopsis

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

## Options

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

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

| Option | Description |
|---|---|
| **-t** | Spécifie le type de certificat à téléverser, à savoir le certificat d'une AC pour le service de répertoire ou le certificat de serveur.<br><br>1 = certificat de serveur<br><br>2 = certificat d'une CA pour le service de répertoire |
| **-f** | Spécifie le nom de fichier du certificat à téléverser. Si le fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné. |

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

## Restrictions

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

## Exemple

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante

---

# sslcertdownload

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-36. sslcertdownload**

| Sous-commande | Description |
|---|---|
| **sslcertupload** | Télécharge un certificat SSL à partir d'iDRAC6 vers le système de fichiers du client. |

## Synopsis

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

## Options

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

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

| Option | Description |
|---|---|
| **-t** | Spécifie le type de certificat à télécharger, à savoir le certificat d'une CA pour le service de répertoire ou le certificat de serveur.<br><br>1 = certificat de serveur<br><br>2 = certificat d'une CA pour le service de répertoire |
| **-f** | Spécifie le nom de fichier du certificat à téléverser. Si l'option **-f** ou le nom de fichier n'est pas spécifié, le fichier **sslcert** présent dans le répertoire actuel est sélectionné. |

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

### Restrictions

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

## Exemple

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante

---

# sslcertview

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-38. sslcertview**

| Sous-commande | Description |
|---|---|
| **sslcertview** | Affiche le serveur SSL ou le certificat d'une AC qui existe sur le RAC. |

## Synopsis

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

## Options

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

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

| Option | Description |
|---|---|
| **-t** | Spécifie le type de certificat à afficher, à savoir le certificat d'une CA ou le certificat du serveur.<br><br>1 = certificat de serveur<br><br>2 = certificat d'une CA pour le service de répertoire |
| **-A** | Empêche d'imprimer les en-têtes/étiquettes. |

## Exemple de sortie

```
racadm sslcertview -t 1

Serial Number             : 00

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

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

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

racadm sslcertview -t 1 -A

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# sslkeyupload

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-40. sslkeyupload**

| Sous-commande | Description |
|---|---|
| **sslkeyupload** | Téléverse la clé SSL du client vers iDRAC6. |

## Synopsis

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

## Options

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

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

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

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

## Restrictions

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

## Exemple

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante

---

# testemail

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

**Tableau A-42.** configuration de testemail

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

## Synopsis

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

## Description

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

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

**Tableau A-43. Configuration de testemail**

| Action | Commande |
|---|---|
| **Activer l'alerte** | racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1 |
| **Définir l'adresse e-mail de destination** | racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 utilisateur1@masociété.com |
| **Définir le message personnalisé qui est envoyé à l'adresse e-mail de destination** | racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "C'est un test !" |
| **Vérifier si l'adresse IP SMTP est configurée correctement** | racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152 |
| **Afficher les paramètres d'alerte par e-mail actuels** | racadm getconfig -g cfgEmailAlert -i <*index*><br><br>où <*index*> est un nombre de 1 à 4 |

## Options

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

**Tableau A-44. Sous-commandes testemail**

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

## Sortie

Aucune.

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# testtrap

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

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

**Tableau A-45. testtrap**

| Sous-commande | Description |
|---|---|
| **testtrap** | Teste la fonctionnalité d'alertes d'interruption SNMP du RAC. |

## Synopsis

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

## Description

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

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

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

**Tableau A-46. Commandes cfgEmailAlert**

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

## Entrée

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

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

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# vmdisconnect

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

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

**Tableau A-48. vmdisconnect**

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

## Synopsis

```
racadm vmdisconnect
```

## Description

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

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# vmkey

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

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

**Tableau A-49. vmkey**

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

## Synopsis

```
racadm vmkey <action>
```

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

## Description

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# usercertupload

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-50. usercertupload**

| Sous-commande | Description |
|---|---|
| **usercertupload** | Téléverse un certificat d'utilisateur ou un certificat AC d'utilisateur du client vers iDRAC6. |

## Synopsis

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

## Options

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

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

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

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

## Restrictions

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

## Exemple

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante

---

# usercertview

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

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

**Tableau A-52. usercertview**

| Sous-commande | Description |
|---|---|
| **usercertview** | Affiche le certificat d'utilisateur ou le certificat AC d'utilisateur qui existe sur iDRAC6. |

## Synopsis

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

## Options

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

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

| Option | Description |
|---|---|
| **-t** | Spécifie le type de certificat à afficher, soit le certificat d'utilisateur, soit le certificat AC d'utilisateur.<br><br>1 = certificat d'utilisateur<br><br>2 = certificat AC d'utilisateur |
| **-A** | Empêche d'imprimer les en-têtes/étiquettes. |
| **-i** | Numéro d'index de l'utilisateur. Valeurs valides : 1-16. |

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

# localConRedirDisable

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

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

**Tableau A-54. localConRedirDisable**

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

## Synopsis

`racadm localConRedirDisable <option>`

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

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

## Interfaces prises en charge

- RACADM locale

---

# krbkeytabupload

**REMARQUE :** Pour utiliser cette commande, vous devez disposer du droit **Configurer iDRAC**.

Le tableau A-55 décrit la sous-commande **krbkeytabupload**.

**Tableau A-55. kerbkeytabupload**

| Sous-commande | Description |
|---|---|
| **krbkeytabupload** | Téléverse le fichier keytab Kerberos. |

## Synopsis

`racadm krbkeytabupload [-f <nom de fichier>]`

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

## Options

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

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

| Option | Description |
|---|---|

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

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

## Restrictions

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

## Exemple

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

## Interfaces prises en charge

- RACADM locale
- RACADM distante

---

# sshpkauth

## Synopsis

```
racadm sshpkauth
```

**Téléversement**

Le mode Téléversement vous permet de téléverser un fichier de clé ou de copier le texte de clé sur la ligne de commande. Vous ne pouvez pas téléverser ni copier une clé simultanément.

RACADM *locale* et *distante :*

```
racadm sshpkauth -i <2 à 16> -k <1 à 4> -f <nom de fichier>
```

RACADM *Telnet/ssh/série:*

```
racadm sshpkauth -i <2 à 16> -k <1 à 4> -t

<texte-clé>
```

**Affichage**

Le mode Affichage permet à l'utilisateur d'afficher une clé spécifiée par l'utilisateur ou toutes les clés.

```
racadm sshpkauth -i <2 à 16> -v -k <1 à 4>

racadm sshpkauth -i <2 à 16> -v -k all
```

**Suppression**

Le mode Suppression permet à l'utilisateur de supprimer une clé spécifiée par l'utilisateur ou toutes les clés.

```
racadm sshpkauth -i <2 à 16> -d -k <1 à 4>

racadm sshpkauth -i <2 à 16> -d -k all
```

## Description

Vous permet de téléverser et de gérer jusqu'à 4 clés publiques SSH différentes. Vous pouvez téléverser un fichier de clé ou afficher une clé spécifiée par l'utilisateur ou toutes les clés, ou encore supprimer une clé spécifiée par l'utilisateur ou toutes les clés. Cette commande intègre trois modes mutuellement exclusifs : Téléversement, Affichage et Suppression déterminés par les options (voir le tableau A-57) fournies à la commande.

## Options

**Tableau A-57. Options de la sous-commande sshpkauth**

| | |
|---|---|

| Option | Description |
|---|---|
| **-i <index utilisateur>** | Index pour l'utilisateur. <index utilisateur> doit être compris entre 2 et 16 sur iDRAC6. |
| **-k [<index de clé> \| all]** | Index d'attribution de la clé PK téléversée. « **all** » fonctionne uniquement avec l'option -v ou -d. <index de clé> doit être compris entre 1 et 4 ou « **all** » sur iDRAC6. |
| **-t <texte de clé PK>** | Texte de clé pour la clé publique SSH. |
| **-f <nom de fichier>** | Fichier contenant le texte de clé à téléverser. L'option **-f** n'est pas prise en charge avec la RACADM Telnet/ssh/série. |
| **-v** | Affichez le texte de clé de l'index fourni. |
| **-d** | Supprimez la clé de l'index fourni. |

## Interfaces prises en charge

- RACADM locale
- RACADM distante
- RACADM Telnet/ssh/série

---

Retour à la page du sommaire

Retour à la page du sommaire

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

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



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

Utilisez les références de groupe et d'objet avec l'utilitaire RACADM pour configurer iDRAC6. Les sections suivantes décrivent chaque objet et indiquent s'il est possible de lire l'objet, d'écrire sur l'objet, ou les deux.

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

Toutes les valeurs de chaîne 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 fournissant des informations sur les spécifications de l'iDRAC6 interrogé.

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

### idRacProductInfo (lecture seule)

#### Valeurs valides

Chaîne de 63 caractères ASCII maximum

#### Valeur par défaut

Integrated Dell Remote Access Controller

### Description

Chaîne de texte qui identifie le produit

## idRacDescriptionInfo (lecture seule)

### Valeurs valides

Chaîne de 255 caractères ASCII maximum

### Valeur par défaut

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

### Description

Description textuelle du type d'iDRAC

## idRacVersionInfo (lecture seule)

### Valeurs valides

Chaîne de 63 caractères ASCII maximum

### Valeur par défaut

<numéro de version actuelle>

### Description

Chaîne de caractères contenant la version actuelle du micrologiciel du produit

## idRacBuildInfo (lecture seule)

### Valeurs valides

Chaîne de 16 caractères ASCII maximum

### Valeur par défaut

Numéro de version actuelle du micrologiciel iDRAC

### Description

Chaîne de caractères contenant le numéro de version actuelle du produit

## idRacName (lecture seule)

### Valeurs valides

Chaîne de 15 caractères ASCII maximum

### Valeur par défaut

iDRAC

### Description

Nom attribué par l'utilisateur pour identifier ce contrôleur

## idRacType (lecture seule)

### Valeurs valides

Référence de produit

### Valeur par défaut

10

### Description

Identifie le type de Remote Access Controller comme iDRAC6.

---

## cfgLanNetworking

Ce groupe contient les paramètres qui permettent de configurer le NIC iDRAC6.

Une seule instance du groupe est autorisée. Certains objets de ce groupe peuvent nécessiter une réinitialisation du NIC iDRAC6, ce qui peut interrompre brièvement la connectivité. Les objets qui modifient les paramètres d'adresse IP du NIC iDRAC6 entraînent la fermeture de toutes les sessions utilisateur actives et imposent aux utilisateurs de se reconnecter en utilisant les paramètres mis à jour de l'adresse IP.

## cfgNicIPv4Enable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Active ou désactive la pile IPv4 iDRAC6

## cfgNicSelection (lecture/écriture)

### Valeurs valides

0 = Partagé

1 = Partagé avec basculement LOM2

2 = Dédié

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

### Valeur par défaut

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

### Description

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

**Tableau B-1. Modes pris en charge par cfgNicSelection**

| Mode | Description |
|---|---|
| Partagé | Utilisé si le NIC intégré du serveur hôte est partagé avec le RAC sur le serveur hôte. Ce mode permet aux configurations d'utiliser la même adresse IP sur le serveur hôte et le RAC pour l'accessibilité commune sur le réseau. |
| Partagé avec basculement : LOM 2 | Active les capacités de regroupement entre les contrôleurs d'interface réseau LOM 2 intégrés du serveur hôte. |
| Dédié | Spécifie que le NIC du RAC est utilisé comme NIC dédié pour l'accessibilité à distance. |
| Partagé avec Basculement : Tous les LOM | Active les capacités de regroupement entre tous les LOM sur les contrôleurs d'interface réseau intégrés du serveur hôte.<br><br>L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via le NIC 1 et le NIC 2, mais transmet des données seulement via le NIC 1. Le basculement se produit du NIC 2 vers le NIC 3 et ensuite vers le NIC 4. Si le NIC 4 est défectueux, le périphérique d'accès à distance rebascule la transmission des données vers le NIC 1, mais uniquement si l'échec initial du NIC 1 a été corrigé. |

## cfgNicVLanEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive les capacités VLAN du RAC/BMC.

## cfgNicVLanId (lecture/écriture)

### Valeurs valides

1 - 4 094

### Valeur par défaut

1

### Description

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

## cfgNicVLanPriority (lecture/écriture)

### Valeurs valides

0 - 7

### Valeur par défaut

0

### Description

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

## cfgDNSDomainNameFromDHCP (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgDNSDomainName (lecture/écriture)

### Valeurs valides

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

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

### Valeur par défaut

<vide>

### Description

Il s'agit du nom de domaine DNS.

## cfgDNSRacName (lecture/écriture)

### Valeurs valides

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

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

### Valeur par défaut

idrac-<numéro de service>

### Description

Affiche le nom de l'iDRAC6, qui est rac-*numéro de service* par défaut. Ce paramètre n'est valide que si **cfgDNSRegisterRac** est défini sur 1 (VRAI).

## cfgDNSRegisterRac (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Enregistre le nom de l'iDRAC6 sur le serveur DNS.

## cfgDNSServersFromDHCP (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgDNSServer1 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

0.0.0.0

### Description

Spécifie l'adresse IPv4 du serveur DNS 1

## cfgDNSServer2 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

0.0.0.0

### Description

Récupère l'adresse IPv4 du serveur DNS 2.

## cfgNicEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

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

## cfgNicIpAddress (lecture/écriture)

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

### Valeurs valides

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

### Valeur par défaut

192.168.0.120

### Description

Spécifie l'adresse IPv4 attribuée à iDRAC6

## cfgNicNetmask (lecture/écriture)

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

### Valeurs valides

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

### Valeur par défaut

255.255.255.0

### Description

Masque de sous-réseau utilisé pour l'adresse IP iDRAC6

## cfgNicGateway (lecture/écriture)

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

### Valeurs valides

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

### Valeur par défaut

192.168.0.1

### Description

Adresse IPv4 de la passerelle iDRAC6

## cfgNicUseDhcp (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Spécifie si DHCP est utilisé pour attribuer l'adresse IPv4 iDRAC6. Si cette propriété est définie sur 1 (VRAI), l'adresse IPv4, le masque de sous-réseau et la passerelle iDRAC6 sont attribués à partir du serveur DHCP sur le réseau. Si cette propriété est définie sur **0** (FAUX), l'utilisateur peut configurer les propriétés **cfgNicIpAddress**, **cfgNicNetmask** et **cfgNicGateway**.

## cfgNicMacAddress (lecture seule)

### Valeurs valides

Chaîne de caractères représentant l'adresse MAC du NIC iDRAC6

### Valeur par défaut

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

### Description

Adresse MAC du NIC iDRAC6

---

## cfgRemoteHosts

Ce groupe fournit des propriétés qui permettent de configurer le serveur SMTP pour les alertes par e-mail.

## cfgRhostsFwUpdateTftpEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Active ou désactive la mise à jour du micrologiciel iDRAC6 à partir d'un serveur TFTP réseau

## cfgRhostsFwUpdateIpAddr (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

0.0.0.0

### Description

Spécifie l'adresse IPv4 du serveur TFTP réseau qui est utilisée pour les opérations de mise à jour du micrologiciel iDRAC6 TFTP.

## cfgRhostsFwUpdatePath (lecture/écriture)

### Valeurs valides

Chaîne de 255 caractères ASCII maximum

### Valeur par défaut

<vide>

### Description

Spécifie le chemin d'accès TFTP où le fichier image du micrologiciel iDRAC6 existe sur le serveur TFTP. Le chemin d'accès TFTP est relatif au chemin d'accès racine TFTP sur le serveur TFTP.

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

## cfgRhostsSmtpServerIpAddr (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

0.0.0.0

### Description

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

## cfgRhostsSyslogEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive le syslog distant.

## cfgRhostsSyslogPort (lecture/écriture)

### Valeurs valides

0 - 65 535

### Valeur par défaut

514

### Description

Numéro de port du syslog distant.

### cfgRhostsSyslogServer1 (lecture/écriture)

#### Valeurs valides

Chaîne de 0 à 254 caractères.

#### Valeur par défaut

<vide>

#### Description

Nom du serveur syslog distant.

### cfgRhostsSyslogServer2 (lecture/écriture)

#### Valeurs valides

Chaîne de 0 à 254 caractères.

#### Valeur par défaut

<vide>

#### Description

Nom du serveur syslog distant.

### cfgRhostsSyslogServer3 (lecture/écriture)

#### Valeurs valides

Chaîne de 0 à 254 caractères.

#### Valeur par défaut

<vide>

#### Description

Nom du serveur syslog distant.

---

## cfgUserAdmin

Ce groupe fournit des informations de configuration sur les utilisateurs qui sont autorisés à accéder à iDRAC6 via les interfaces à distance disponibles.

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

### cfgUserAdminIndex (lecture seule)

### Valeurs valides

1 - 16

### Valeur par défaut

<instance>

### Description

Ce nombre représente l'instance de l'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 maximal 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 d'autorité basés sur le rôle qui sont autorisés pour l'utilisateur. La valeur est représentée comme un masque binaire qui autorise n'importe quelle combinaison de valeurs de privilège. Le tableau B-2 décrit les valeurs binaires des privilèges utilisateur pouvant être combinées pour créer des masques binaires.

**Tableau B-2. Masques binaires pour les privilèges utilisateur**

| Privilège utilisateur | Masque binaire de privilège |
|---|---|
| Ouvrir une session sur iDRAC | 0x00000001 |
| Configurer iDRAC | 0x00000002 |
| Configurer les utilisateurs | 0x00000004 |

| | |
|---|---|
| Effacer les journaux | 0x00000008 |
| Exécuter les commandes de contrôle du serveur | 0x00000010 |
| Accéder à la redirection de console | 0x00000020 |
| Accéder au média virtuel | 0x00000040 |
| Tester les alertes | 0x00000080 |
| Exécuter les commandes de débogage | 0x00000100 |

### Exemples

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

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

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

## cfgUserAdminUserName (lecture/écriture)

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

### Valeurs valides

Chaîne de 16 caractères ASCII maximum

### Valeur par défaut

racine (utilisateur 2)

<vide> (tous les autres)

### Description

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 au niveau de cet index. La chaîne de caractères ne peut pas contenir de barre oblique (/), de barre oblique inverse (\), de point (.), d'arobase (@) ou de guillemets.

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

## cfgUserAdminPassword (lecture seule)

### Valeurs valides

Chaîne de 20 caractères ASCII maximum

### Valeur par défaut

********

### Description

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

## cfgUserAdminEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1 (utilisateur 2)

0 (tous les autres)

### Description

Active ou désactive un utilisateur individuel

## cfgUserAdminSolEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgUserAdminIpmiSerialPrivilege (lecture/écriture)

### Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

15 (pas d'accès)

### Valeur par défaut

4 (utilisateur 2)

15 (tous les autres)

### Description

### Privilège maximal sur le canal LAN IPMI

## cfgEmailAlert

Ce groupe contient des paramètres pour configurer les capacités d'alerte par e-mail iDRAC6.

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

### cfgEmailAlertIndex (lecture seule)

#### Valeurs valides

1-4

#### Valeur par défaut

<instance>

#### Description

Index unique d'une instance d'alerte

### cfgEmailAlertEnable (lecture/écriture)

#### Valeurs valides

1 (VRAI)

0 (FAUX)

#### Valeur par défaut

0

#### Description

Active ou désactive l'instance d'alerte

### cfgEmailAlertAddress (lecture/écriture)

#### Valeurs valides

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

#### Valeur par défaut

<vide>

#### Description

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

## cfgEmailAlertCustomMsg (lecture/écriture)

### Valeurs valides

Chaîne de 32 caractères maximum

### Valeur par défaut

<vide>

### Description

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

---

# cfgSessionManagement

Ce groupe contient les paramètres de configuration du nombre de sessions qui peuvent se connecter à iDRAC6.

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

## cfgSsnMgtRacadmTimeout (lecture/écriture)

### Valeurs valides

10 - 1 920

### Valeur par défaut

60

### Description

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

## cfgSsnMgtConsRedirMaxSessions (lecture/écriture)

### Valeurs valides

1 - 4

### Valeur par défaut

4

### Description

Spécifie le nombre maximal de sessions de redirection de console autorisées sur iDRAC6

## cfgSsnMgtWebserverTimeout (lecture/écriture)

### Valeurs valides

60 - 10 800

### Valeur par défaut

1 800

### Description

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

## cfgSsnMgtSshIdleTimeout (lecture/écriture)

### Valeurs valides

0 (pas de délai d'attente)

60 - 1 920

### Valeur par défaut

300

### Description

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

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

```
Connection timed out (La connexion a expiré)
```

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

## cfgSsnMgtTelnetTimeout (lecture/écriture)

### Valeurs valides

0 (pas de délai d'attente)

60 - 1 920

### Valeur par défaut

300

### Description

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

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

```
Connection timed out (La connexion a expiré)
```

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

## cfgSerial

Ce groupe contient les paramètres de configuration des services iDRAC6.

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

### cfgSerialBaudRate (lecture/écriture)

#### Valeurs valides

9 600, 28 800, 57 600, 115 200

#### Valeur par défaut

57 600

#### Description

Définit le débit en bauds du port série iDRAC6.

### cfgSerialConsoleEnable (lecture/écriture)

#### Valeurs valides

1 (VRAI)

0 (FAUX)

#### Valeur par défaut

0

#### Description

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

### cfgSerialConsoleQuitKey (lecture/écriture)

#### Valeurs valides

Chaîne de 4 caractères maximum

#### Valeur par défaut

^\ (<Ctrl><\>)

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

#### Description

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

- Valeur décimale - Par exemple : « 95 »

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

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

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

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

## cfgSerialConsoleIdleTimeout (lecture/écriture)

### Valeurs valides

0 = aucun délai d'attente

60 - 1 920

### Valeur par défaut

300

### Description

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

## cfgSerialConsoleNoAuth (lecture/écriture)

### Valeurs valides

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

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

### Valeur par défaut

0

### Description

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

## cfgSerialConsoleCommand (lecture/écriture)

### Valeurs valides

Chaîne de 128 caractères maximum.

### Valeur par défaut

<vide>

### Description

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

## cfgSerialHistorySize (lecture/écriture)

### Valeurs valides

0 - 8 192

### Valeur par défaut

8 192

### Description

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

## cfgSerialCom2RedirEnable (lecture/écriture)

### Valeur par défaut

1

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Description

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

## cfgSerialSshEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

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

## cfgSerialTelnetEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive l'interface de console Telnet sur iDRAC6

---

## cfgOobSnmp

Ce groupe contient des paramètres de configuration de l'agent SNMP et des capacités d'interruption de l'iDRAC6.

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

## cfgOobSnmpAgentCommunity (lecture/écriture)

### Valeurs valides

Chaîne de 31 caractères maximum

### Valeur par défaut

public

### Description

Spécifie le nom de communauté SNMP utilisé pour les interruptions SNMP

## cfgOobSnmpAgentEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive l'agent SNMP dans iDRAC6

---

## cfgRacTuning

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

## cfgRacTuneConRedirPort (lecture/écriture)

### Valeurs valides

1 - 65 535

### Valeur par défaut

5 900

### Description

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

## cfgRacTuneRemoteracadmEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Active ou désactive l'interface RACADM distante dans iDRAC

## cfgRacTuneCtrlEConfigDisable

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgRacTuneHttpPort (lecture/écriture)

### Valeurs valides

1 - 65 535

### Valeur par défaut

80

### Description

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

## cfgRacTuneHttpsPort (lecture/écriture)

### Valeurs valides

1 - 65 535

### Valeur par défaut

443

### Description

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

## cfgRacTuneIpRangeEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive la fonctionnalité de validation de la plage d'adresses IPv4 de l'iDRAC6

## cfgRacTuneIpRangeAddr (lecture/écriture)

### Valeurs valides

Une chaîne d'adresse IPv4 formatée, par exemple 192.168.0.44

### Valeur par défaut

192.168.1.1

### Description

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

## cfgRacTuneIpRangeMask (lecture/écriture)

### Valeurs valides

Chaîne d'adresse IPv4 formatée, par exemple `255.255.255.0`

### Valeur par défaut

255.255.255.0

### Description

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

## cfgRacTuneIpBlkEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive la fonctionnalité de blocage de l'adresse IPv4 de l'iDRAC6

## cfgRacTuneIpBlkFailCount (lecture/écriture)

### Valeurs valides

2 - 16

### Valeur par défaut

5

### Description

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

## cfgRacTuneIpBlkFailWindow (lecture/écriture)

### Valeurs valides

10 - 65 535

### Valeur par défaut

60

### Description

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

## cfgRacTuneIpBlkPenaltyTime (lecture/écriture)

### Valeurs valides

10 - 65 535

### Valeur par défaut

300

### Description

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

## cfgRacTuneSshPort (lecture/écriture)

### Valeurs valides

1 - 65 535

### Valeur par défaut

22

### Description

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

## cfgRacTuneTelnetPort (lecture/écriture)

### Valeurs valides

1 - 65 535

### Valeur par défaut

23

### Description

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

## cfgRacTuneConRedirEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Active la redirection de console

## cfgRacTuneConRedirEncryptEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Crypte la vidéo dans une session de redirection de console

## cfgRacTuneAsrEnable (lecture/écriture)

**REMARQUE :** Cet objet nécessite une réinitialisation de l'iDRAC6 pour devenir actif.

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgRacTuneDaylightOffset (lecture/écriture)

### Valeurs valides

0 - 60

### Valeur par défaut

0

### Description

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

## cfgRacTuneTimezoneOffset (lecture/écriture)

### Valeurs valides

-720 - 780

### Valeur par défaut

0

### Description

Spécifie le décalage de fuseau horaire (en minutes) par rapport au temps moyen de Greenwich/temps universel coordonné à utiliser pour l'heure du RAC. Certains décalages de fuseau horaire courants pour les fuseaux horaires des États-Unis sont affichés ci-dessous :

-480 (PST : heure normale du Pacifique)

-420 (MST : heure normale des Rocheuses)

-360 (CST : heure normale du Centre)

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

## cfgRacTuneLocalServerVideo (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

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

## cfgRacTuneLocalConfigDisable (lecture/écriture)

### Valeurs valides

0 (VRAI)

1 (FAUX)

### Valeur par défaut

0

### Description

Désactive l'accès en écriture aux données de configuration iDRAC6 en le définissant sur 1

## cfgRacTuneWebserverEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Active ou désactive le serveur Web 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 Telnet/SSH ou RACADM.

---

## ifcRacManagedNodeOs

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

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

## ifcRacMnOsHostname (lecture seule)

### Valeurs valides

Chaîne de 255 caractères maximum

### Valeur par défaut

<vide>

### Description

Nom d'hôte du serveur géré

## ifcRacMnOsOsName (lecture seule)

### Valeurs valides

Chaîne de 255 caractères maximum

### Valeur par défaut

<vide>

### Description

Nom du système d'exploitation du serveur géré

---

## cfgRacSecurity

Ce groupe est utilisé pour configurer les paramètres relatifs à la fonctionnalité de requête de signature de certificat (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.

## cfgRacSecCsrCommonName (lecture/écriture)

### Valeurs valides

Chaîne de 254 caractères maximum

### Valeur par défaut

<vide>

### Description

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

## cfgRacSecCsrOrganizationName (lecture/écriture)

### Valeurs valides

Chaîne de 254 caractères maximum

### Valeur par défaut

<vide>

### Description

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

## cfgRacSecCsrOrganizationUnit (lecture/écriture)

### Valeurs valides

Chaîne de 254 caractères maximum

### Valeur par défaut

<vide>

### Description

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

## cfgRacSecCsrLocalityName (lecture/écriture)

### Valeurs valides

Chaîne de 254 caractères maximum

### Valeur par défaut

<vide>

### Description

Spécifie la ville (L) de la RSC

## cfgRacSecCsrStateName (lecture/écriture)

### Valeurs valides

Chaîne de 254 caractères maximum

### Valeur par défaut

<vide>

### Description

Spécifie le nom d'état (S) de la RSC

## cfgRacSecCsrCountryCode (lecture/écriture)

### Valeurs valides

Chaîne de 2 caractères maximum

### Valeur par défaut

<vide>

### Description

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

## cfgRacSecCsrEmailAddr (lecture/écriture)

### Valeurs valides

Chaîne de 254 caractères maximum

### Valeur par défaut

<vide>

### Description

Spécifie l'adresse e-mail de la RSC

## cfgRacSecCsrKeySize (lecture/écriture)

### Valeurs valides

1 024

2 048

4 096

### Valeur par défaut

1 024

### 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.

## cfgRacVirMediaAttached (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 connectés, le serveur reconnaît les périphériques de stockage de masse USB valides connectés au système. Cela revient à connecter un lecteur de CD-ROM/disquette USB local à un port USB sur le système. Lorsque les périphériques sont connectés, 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 sont déconnectés du bus USB.

## cfgVirMediaBootOnce (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive la fonctionnalité de **démarrage unique de média virtuel** iDRAC6.

## cfgVirtualFloppyEmulation (lecture/écriture)

**REMARQUE :** Le média virtuel doit être reconnecté (à l'aide de cfgRacVirMediaAttached) pour que cette modification prenne effet.

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgVirMediaKeyEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgSDWriteProtect (lecture seule)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

---

## cfgServerInfo

Ce groupe vous permet de sélectionner le périphérique de démarrage initial du BIOS et de démarrer le périphérique sélectionné une seule fois.

## cfgServerFirstBootDevice (lecture/écriture)

### Valeurs valides

No-Override

PXE

HDD

DIAG

CD-DVD

BIOS

vFDD

VCD-DVD

iSCSI

VFLASH

FDD

SD

### Valeur par défaut

No-Override

### Description

Définit ou affiche le périphérique de démarrage initial.

## cfgServerBootOnce (lecture/écriture)

### Valeurs valides

1 = VRAI

0 = FAUX

### Valeur par défaut

0

### Description

Active ou désactive la fonctionnalité de démarrage unique du serveur.

---

## 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 contenant jusqu'à 254 caractères, avec ou sans espace

### Valeur par défaut

<vide>

### Description

Domaine Active Directory dans lequel se trouve iDRAC6

## cfgADRacName (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

Nom de l'iDRAC6 enregistré dans la forêt Active Directory

## cfgADEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgADSSOEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive l'authentification par connexion directe Active Directory sur iDRAC6.

## cfgADDomainController1 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

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

## cfgADDomainController2 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

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

## cfgADDomainController3 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

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

## cfgADAuthTimeout (lecture/écriture)

### Valeurs valides

15 - 300 secondes

### Valeur par défaut

120

### Description

Spécifie le nombre de secondes à attendre pour que les requêtes d'authentification Active Directory soient exécutées avant l'expiration du délai.

## cfgADType (lecture/écriture)

### Valeurs valides

1 (schéma étendu)

2 (schéma standard)

### Valeur par défaut

1

### Description

Détermine le type de schéma à utiliser avec Active Directory

## cfgADGlobalCatalog1 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

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

## cfgADGlobalCatalog2 (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

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

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

### Valeur par défaut

<vide>

### Description

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

## cfgADCertValidationEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

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

## cfgADDcSRVLookupEnable (lecture/écriture)

### Valeurs valides

1 (VRAI) : utilisez DNS pour rechercher les contrôleurs de domaine

0 (FAUX) : utilisez les contrôleurs de domaine préconfigurés

### Valeur par défaut

0

### Définition

Configure iDRAC6 pour utiliser les contrôleurs de domaine préconfigurés ou pour utiliser DNS afin de trouver le contrôleur de domaine. Si vous utilisez des contrôleurs de domaine préconfigurés, les contrôleurs de domaine à utiliser sont alors spécifiés sous cfgAdDomainController1, cfgAdDomainController2 et cfgAdDomainController3. iDRAC6 ne bascule pas sur les contrôleurs de domaine spécifiés lorsque la recherche DNS échoue, sinon aucun des serveurs renvoyés par la recherche DNS ne fonctionnerait.

## cfgADDcSRVLookupbyUserdomain (lecture/écriture)

### Valeurs valides

1 (VRAI) : utilisez le domaine d'utilisateur en tant que domaine de recherche pour rechercher les contrôleurs de domaine. Le domaine d'utilisateur est sélectionné dans la liste de domaines d'utilisateur ou saisi par l'utilisateur d'ouverture de session.

0 (FAUX) : utilisez le domaine de recherche configuré *cfgADDcSrvLookupDomainName* pour rechercher les contrôleurs de domaine.

### Valeur par défaut

1

### Définition

Spécifie la façon dont le domaine d'utilisateur est recherché pour Active Directory.

## cfgADDcSRVLookupDomainName (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

### Définition

Il s'agit du domaine Active Directory à utiliser lorsque *cfgAddcSrvLookupbyUserDomain* est défini sur 0.

## cfgADGcSRVLookupEnable (lecture/écriture)

### Valeurs valides

0 (FAUX) : utilisez les serveurs de catalogue global (SCG) préconfigurés

1 (VRAI) : utilisez DNS pour rechercher les SCG

### Valeur par défaut

0

### Définition

Détermine la façon dont le serveur de catalogue global est recherché. Si vous utilisez des serveurs de catalogue global préconfigurés, iDRAC6 utilise alors les valeurs cfgAdGlobalCatalog1, cfgAdGlobalCatalog2 et cfgAdGlobalCatalog3.

## cfgADGcRootDomain (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

### Description

Nom du domaine racine Active Directory utilisé pour la recherche DNS, pour localiser les serveurs de catalogue global.

---

# cfgLDAP

Ce groupe vous permet de configurer les paramètres relatifs au protocole LDAP (Lightweight Directory Access Protocol).

## cfgLdapEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive le service LDAP.

## cfgLdapServer (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 1 024

### Valeur par défaut

Null

### Description

Configure l'adresse du serveur LDAP.

## cfgLdapPort (lecture/écriture)

### Valeurs valides

1 - 65 535

### Valeur par défaut

636

### Description

Port de LDAP sur SSL. Tout port autre que SSL n'est pas pris en charge.

## cfgLdapBasedn (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

### Description

Nom de domaine de la branche du répertoire à partir duquel toutes les recherches doivent débuter.

## cfgLdapUserAttribute (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

*uid* en cas de non configuration.

### Description

Spécifie l'attribut d'utilisateur à rechercher. S'il n'est pas configuré, uid est utilisé par défaut. Il est recommandé de veiller à ce qu'il soit unique dans le nom unique de base choisi, sinon un filtre de recherche doit être configuré afin de garantir l'unicité de l'utilisateur d'ouverture de session. Si le nom unique d'utilisateur ne peut pas être identifié de manière unique, l'ouverture de session échouera et une erreur sera générée.

## cfgLdapGroupAttribute (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

### Description

Spécifiez quel attribut LDAP est utilisé pour vérifier l'appartenance au groupe. Il doit s'agir d'un attribut de la classe de groupe. S'il n'est pas spécifié, iDRAC6 utilise le membre et les attributs de membre uniques.

## cfgLdapGroupAttributeIsDN (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Lorsqu'il est défini sur 1, iDRAC6 compare le nom unique d'utilisateur récupéré dans le répertoire aux membres du groupe ; s'il est défini sur 0, le nom d'utilisateur fourni par l'utilisateur d'ouverture de session sera utilisé en vue de la comparaison avec les membres du groupe. Cette action n'a aucune incidence sur l'algorithme de recherche de la liaison. iDRAC6 recherche toujours le nom unique d'utilisateur et l'utilise pour établir la liaison.

## cfgLdapBinddn (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

### Description

Le nom unique d'un utilisateur utilisé pour établir la liaison au serveur lors de la recherche du nom unique de l'utilisateur d'ouverture de session. S'il n'est pas fourni, une liaison anonyme est utilisée. Ceci est facultatif mais requis si la liaison anonyme n'est pas prise en charge.

## cfgLdapBindpassword (écriture seule)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

Null

### Description

Mot de passe de liaison à utiliser conjointement avec le nom unique de liaison. Le mot de passe de liaison contient des données sensibles et doit être protégé de manière appropriée. Ceci est facultatif mais requis si la liaison anonyme n'est pas prise en charge.

## cfgLdapSearchFilter (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 254

### Valeur par défaut

(classe d'objet=*)

Recherche tous les objets dans l'arborescence.

### Description

Filtre de recherche LDAP valide. Ceci est utilisé si l'attribut d'utilisateur ne parvient pas à identifier de manière unique l'utilisateur d'ouverture de session dans le nom unique de base choisi. Le « filtre de recherche » s'applique uniquement à la recherche du nom unique d'utilisateur, et non à la recherche d'appartenance au groupe.

## cfgLDAPCertValidationEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Contrôle la validation de certificat lors de l'établissement de liaisons SSL.

---

# cfgLdapRoleGroup

Ce groupe permet à l'utilisateur de configurer les groupes de rôles pour LDAP.

## cfgLdapRoleGroupIndex (lecture seule)

### Valeurs valides

Nombre entier compris entre 1 et 5

### Valeur par défaut

<instance>

### Description

Il s'agit de la valeur d'index de l'objet Groupe de rôles.

## cfgLdapRoleGroupDN (lecture/écriture)

### Valeurs valides

Chaîne de caractères. Longueur maximale = 1 024

### Valeur par défaut

<vide>

### Description

Il s'agit du nom de domaine du groupe dans cet index.

## cfgLdapRoleGroupPrivilege (lecture/écriture)

### Valeurs valides

0x00000000 à 0x000001ff

### Valeur par défaut

0x000

### Description

Masque binaire définissant les privilèges associés à ce groupe spécifique.

---

# cfgStandardSchema

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

## cfgSSADRoleGroupIndex (lecture seule)

### Valeurs valides

Nombre entier compris entre 1 et 5

### Valeur par défaut

<instance>

### Description

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

## cfgSSADRoleGroupName (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

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

## cfgSSADRoleGroupDomain (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

<vide>

### Description

Domaine Active Directory dans lequel se trouve le groupe de rôles

## cfgSSADRoleGroupPrivilege (lecture/écriture)

### Valeurs valides

**0x00000000** à **0x000001ff**

### Valeur par défaut

<vide>

### Description

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

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

| Privilèges de groupes de rôles | Masque binaire |
|---|---|
| Ouvrir une session sur iDRAC | 0x00000001 |
| Configurer iDRAC | 0x00000002 |
| Configurer les utilisateurs | 0x00000004 |
| Effacer les journaux | 0x00000008 |
| Exécuter les commandes de contrôle du serveur | 0x00000010 |
| Accéder à la redirection de console | 0x00000020 |

| | |
|---|---|
| Accéder au média virtuel | 0x00000040 |
| Tester les alertes | 0x00000080 |
| Exécuter les commandes de débogage | 0x00000100 |

---

## cfgIpmiSol

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

### cfgIpmiSolEnable (lecture/écriture)

#### Valeurs valides

1 (VRAI)

0 (FAUX)

#### Valeur par défaut

1

#### Description

Active ou désactive SOL

### cfgIpmiSolBaudRate (lecture/écriture)

#### Valeurs valides

9 600, 19 200, 57 600, 115 200

#### Valeur par défaut

115 200

#### Description

Débit en bauds pour les communications série sur le LAN

### cfgIpmiSolMinPrivilege (lecture/écriture)

#### Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

#### Valeur par défaut

4

### Description

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

## cfgIpmiSolAccumulateInterval (lecture/écriture)

### Valeurs valides

1 - 255

### Valeur par défaut

10

### Description

Spécifie le temps type pendant lequel iDRAC6 attend avant de transmettre un paquet de données de caractères SOL partiel. Cette valeur est basée sur des incréments de 5 ms de 1.

## cfgIpmiSolSendThreshold (lecture/écriture)

### Valeurs valides

1 - 255

### Valeur par défaut

255

### Description

Valeur seuil SOL. Spécifie le nombre maximal 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 LAN du système.

## cfgIpmiLanEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive l'interface IPMI sur LAN.

## cfgIpmiLanPrivilegeLimit (lecture/écriture)

### Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

### Valeur par défaut

4

### Description

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

## cfgIpmiLanAlertEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

## cfgIpmiEncryptionKey (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

00000000000000000000

### Description

Clé de cryptage IPMI.

## cfgIpmiPetCommunityName (lecture/écriture)

### Valeurs valides

Chaîne allant jusqu'à 18 caractères

### Valeur par défaut

public

### Description

Nom de communauté SNMP pour les interruptions

---

## cfgIpmiPetIpv6

Ce groupe est utilisé pour configurer les interruptions d'événements sur plateforme IPv6 sur le serveur géré.

## cfgIpmiPetIPv6Index (lecture seule)

### Valeurs valides

1 - 4

### Valeur par défaut

<valeur d'index>

### Description

Identifiant unique pour l'index correspondant à l'interruption

## cfgIpmiPetIPv6AlertDestIpAddr

### Valeurs valides

Adresse IPv6

### Valeur par défaut

<vide>

### Description

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

## cfgIpmiPetIPv6AlertEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

---

## cfgIpmiPef

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

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

Pour configurer l'action PEF du filtre d'assertion d'informations de la carte SD, vous ne pouvez pas utiliser la commande racadm locale. Utilisez plutôt la commande racadm distante :

```
racadm -r <adresse ip iDRAC6> -u <nom d'utilisateur> -p <calvin> config -g cfgIpmipef -i 20 -o cfgIpmipefaction [0-3]
```

## cfgIpmiPefName (lecture seule)

### Valeurs valides

Chaîne de 255 caractères maximum

### Valeur par défaut

Nom du filtre d'index

### Description

Spécifie le nom du filtre d'événements sur plateforme

## cfgIpmiPefIndex (lecture/écriture)

### Valeurs valides

1 - 22

### Valeur par défaut

Valeur d'index d'un objet 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

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

Active ou désactive un filtre d'événements sur plateforme spécifique

---

## cfgIpmiPet

Ce groupe est utilisé pour configurer les interruptions d'événements sur plateforme sur le serveur géré.

## cfgIpmiPetIndex (lecture seule)

### Valeurs valides

1 - 4

### Valeur par défaut

Valeur d'index d'une interruption d'événements sur plateforme spécifique

### Description

Identifiant unique pour l'index correspondant à l'interruption

## cfgIpmiPetAlertDestIpAddr (lecture/écriture)

### Valeurs valides

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

### Valeur par défaut

0.0.0.0

### Description

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

## cfgIpmiPetAlertEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

Active ou désactive une interruption spécifique

---

## cfgUserDomain

Ce groupe est utilisé pour configurer les noms de domaine utilisateur Active Directory. Un maximum de 40 noms de domaine peut être configuré à un moment donné.

## cfgUserDomainIndex (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

Valeur d'index

### Description

Représente un domaine spécifique

## cfgUserDomainName (lecture seule)

### Valeurs valides

Chaîne de 255 caractères ASCII maximum

### Valeur par défaut

<vide>

### Description

Spécifie le nom de domaine utilisateur Active Directory

---

## cfgServerPower

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

### cfgServerPowerStatus (lecture seule)

#### Valeurs valides

1 (MARCHE)

0 (ARRÊT)

#### Valeur par défaut

<état d'alimentation actuel du serveur>

#### Description

Représente l'état d'alimentation du serveur (MARCHE ou ARRÊT)

### cfgServerPowerServerAllocation (lecture seule)

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

#### Valeurs valides

Chaîne de 32 caractères maximum

#### Valeur par défaut

<vide>

#### Description

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

### cfgServerActualPowerConsumption (lecture seule)

#### Valeurs valides

Chaîne de 32 caractères maximum

#### Valeur par défaut

<vide>

### Description

Représente la consommation actuelle du serveur

## cfgServerPowerCapEnable (lecture seule)

### Valeurs valides

0

1

### Valeur par défaut

1

### Description

Active ou désactive le seuil du bilan de puissance spécifié par l'utilisateur

## cfgServerMinPowerCapacity (lecture seule)

### Valeurs valides

Chaîne de 32 caractères maximum

### Valeur par défaut

<vide>

### Description

Représente la capacité d'alimentation minimale du serveur

## cfgServerMaxPowerCapacity (lecture seule)

### Valeurs valides

Chaîne de 32 caractères maximum

### Valeur par défaut

<vide>

### Description

Représente la capacité d'alimentation maximale du serveur

## cfgServerPeakPowerConsumption (lecture seule)

### Valeurs valides

Chaîne de 32 caractères maximum

### Valeur par défaut

<consommation énergétique maximale actuelle du serveur>

### Description

Représente la consommation maximale du serveur jusqu'à présent

## cfgServerPeakPowerConsumptionTimestamp (lecture seule)

### Valeurs valides

Chaîne de 32 caractères maximum

### Valeur par défaut

Horodatage de la consommation énergétique maximale

### Description

Heure à laquelle la consommation électrique maximale a été enregistrée

## cfgServerPowerConsumptionClear (lecture seule)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

*******

### Description

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

## cfgServerPowerCapWatts (lecture/écriture)

### Valeurs valides

Chaîne de 32 caractères maximum

### Valeur par défaut

Seuil énergétique du serveur en watts

#### Description

Représente le seuil énergétique du serveur en watts

### cfgServerPowerCapBtuhr (lecture/écriture)

#### Valeurs valides

Chaîne de 32 caractères maximum

#### Valeur par défaut

Seuil énergétique du serveur en BTU/h

#### Description

Représente le seuil énergétique du serveur en BTU/h

### cfgServerPowerCapPercent (lecture/écriture)

#### Valeurs valides

Chaîne de 32 caractères maximum

#### Valeur par défaut

Seuil énergétique du serveur en pourcentage

#### Description

Représente le seuil énergétique du serveur en pourcentage

---

## cfgIPv6LanNetworking

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

### cfgIPv6Enable

#### Valeurs valides

1 (VRAI)

0 (FAUX)

#### Valeur par défaut

0

#### Description

Active ou désactive la pile IPv6 iDRAC6

## cfgIPv6Address1 (lecture/écriture)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

::

### Description

## Adresse IPv6 iDRAC6

## cfgIPv6Gateway (lecture/écriture)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

::

### Description

Adresse IPv6 de la passerelle iDRAC6

## cfgIPv6PrefixLength (lecture/écriture)

### Valeurs valides

1-128

### Valeur par défaut

64

## Description

Longueur de préfixe pour l'adresse 1 IPv6 iDRAC6

## cfgIPv6AutoConfig (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

## Description

Active ou désactive l'option Config auto IPv6

## cfgIPv6LinkLocalAddress (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

::

## Description

Adresse locale de liaison IPv6 iDRAC6

## cfgIPv6Address2 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

::

## Description

Adresse IPv6 iDRAC6

## cfgIPv6DNSServersFromDHCP6 (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

## Description

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

## cfgIPv6DNSServer1 (lecture/écriture)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

::

## Description

Adresse IPV6 du serveur DNS

## cfgIPv6DNSServer2 (lecture/écriture)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

::

## Description

Adresse IPV6 du serveur DNS

## cfgIPv6Addr2PrefixLength (lecture seule)

### Valeurs valides

1-128

### Valeur par défaut

0

### Description

Longueur de préfixe pour l'adresse 2 IPv6 iDRAC6

## cfgIPv6LinkLockPrefixLength (lecture seule)

### Valeurs valides

1-128

### Valeur par défaut

0

## cfgTotalnumberofextended IP (lecture/écriture)

### Valeurs valides

1 - 256

### Valeur par défaut

<vide>

## cfgIPv6Addr3PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

<vide>

## cfgIPv6Addr3Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address3 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr4PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr4Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address4 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr5PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr5Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address5 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr6PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr6Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address6 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr7PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr7Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address7 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr8PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr8Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address8 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr9PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr9Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address9 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr10PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr10Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address10 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr11PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr11Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address11 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr12PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr12Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address12 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr13PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr13Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address13 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr14PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr14Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address14 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

## cfgIPv6Addr15PrefixLength (lecture seule)

### Valeurs valides

1 - 128

### Valeur par défaut

0

## cfgIPv6Addr15Length (lecture seule)

### Valeurs valides

1 - 40

### Valeur par défaut

<vide>

## cfgIPv6Address15 (lecture seule)

### Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide

### Valeur par défaut

<vide>

---

## cfgIPv6URL

Ce groupe spécifie les propriétés utilisées pour configurer l'URL IPv6 iDRAC6.

## cfgIPv6URLstring (lecture seule)

### Valeurs valides

Chaîne de 80 caractères maximum

### Valeur par défaut

<vide>

### Description

URL IPv6 iDRAC6

---

## cfgIpmiSerial

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

## cfgIpmiSerialConnectionMode (lecture/écriture)

### Valeurs valides

0 (terminal)

1 (de base)

### Valeur par défaut

1

### Description

Lorsque la propriété **cfgSerialConsoleEnable** iDRAC6 est définie sur 0 (désactivé), le port série iDRAC6 devient le port série IPMI. Cette propriété détermine le mode défini IPMI du port série.

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

## cfgIpmiSerialBaudRate (lecture/écriture)

### Valeurs valides

9 600, 19 200, 57 600, 115 200

### Valeur par défaut

57 600

### Description

Spécifie le débit en bauds pour une connexion série sur IPMI

## cfgIpmiSerialChanPrivLimit (lecture/écriture)

### Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

### Valeur par défaut

4

### Description

Spécifie le niveau de privilège maximal autorisé sur le canal série IPMI

## cfgIpmiSerialFlowControl (lecture/écriture)

### Valeurs valides

0 (aucun)

1 (CTS/RTS)

2 (XON/XOFF)

### Valeur par défaut

1

### Description

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

## cfgIpmiSerialHandshakeControl (lecture/écriture)

### Valeurs valides

0 (FAUX)

1 (VRAI)

### Valeur par défaut

1

### Description

Active ou désactive le contrôle d'établissement de liaisons du mode terminal IPMI

## cfgIpmiSerialLineEdit (lecture/écriture)

### Valeurs valides

0 (FAUX)

1 (VRAI)

### Valeur par défaut

1

### Description

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

## cfgIpmiSerialEchoControl (lecture/écriture)

### Valeurs valides

0 (FAUX)

1 (VRAI)

### Valeur par défaut

1

### Description

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

## cfgIpmiSerialDeleteControl (lecture/écriture)

### Valeurs valides

0 (FAUX)

1 (VRAI)

### Valeur par défaut

0

### Description

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

## cfgIpmiSerialNewLineSequence (lecture/écriture)

### Valeurs valides

0 (aucun)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

### Valeur par défaut

1

### Description

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

## cfgIpmiSerialInputNewLineSequence (lecture/écriture)

### Valeurs valides

0 (<ENTRÉE>)

1 (NULL)

### Valeur par défaut

1

### Description

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

---

# cfgSmartCard

Ce groupe spécifie les propriétés utilisées pour prendre en charge l'accès à iDRAC6 au moyen d'une carte à puce.

## cfgSmartCardLogonEnable (lecture/écriture)

### Valeurs valides

0 (désactivé)

1 (activé)

2 (activé avec la RACADM distante)

### Valeur par défaut

0

### Description

Active, désactive ou active avec la RACADM distante la prise en charge de l'accès à iDRAC6 au moyen d'une carte à puce.

## cfgSmartCardCRLEnable (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

0

### Description

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

---

## cfgNetTuning

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

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

## cfgNetTuningNicAutoneg (lecture/écriture)

### Valeurs valides

1 (VRAI)

0 (FAUX)

### Valeur par défaut

1

### Description

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

## cfgNetTuningNic100MB (lecture/écriture)

### Valeurs valides

0 (10 Mb)

1 (100 Mb)

### Valeur par défaut

1

### Description

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

## cfgNetTuningNicFullDuplex (lecture/écriture)

### Valeurs valides

0 (semi-duplex)

1 (duplex intégral)

### Valeur par défaut

1

### Description

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

## cfgNetTuningNicMtu (lecture/écriture)

### Valeurs valides

576 - 1 500

### Valeur par défaut

1 500

### Description

La taille en octets de l'unité de transmission maximale utilisée par le NIC iDRAC6.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Interfaces RACADM prises en charge

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**

Le tableau C-1 présente les sous-commandes RACADM et leur prise en charge d'interface correspondante.

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

| Sous-commande | Telnet/SSH/série | RACADM locale | RACADM distante |
|---|---|---|---|
| arp | ✓ | ✗ | ✓ |
| clearasrscreen | ✓ | ✓ | ✓ |
| clrraclog | ✓ | ✓ | ✓ |
| clrsel | ✓ | ✓ | ✓ |
| coredump | ✓ | ✗ | ✓ |
| coredumpdelete | ✓ | ✓ | ✓ |
| fwupdate | ✓ | ✓ | ✓ |
| getconfig | ✓ | ✓ | ✓ |
| getniccfg | ✓ | ✓ | ✓ |
| getraclog | ✓ | ✓ | ✓ |
| getractime | ✓ | ✓ | ✓ |
| getsel | ✓ | ✓ | ✓ |
| getssninfo | ✓ | ✓ | ✓ |
| getsvctag | ✓ | ✓ | ✓ |
| getsysinfo | ✓ | ✓ | ✓ |
| gettracelog | ✓ | ✓ | ✓ |
| help | ✓ | ✓ | ✓ |
| ifconfig | ✓ | ✗ | ✓ |
| krbkeytabupload | ✗ | ✓ | ✓ |
| netstat | ✓ | ✗ | ✓ |
| ping | ✓ | ✗ | ✓ |
| racdump | ✓ | ✗ | ✓ |
| racreset | ✓ | ✓ | ✓ |
| racresetcfg | ✓ | ✓ | ✓ |
| serveraction | ✓ | ✓ | ✓ |
| setniccfg | ✓ | ✓ | ✓ |
| sshpkauth | ✓ | ✓ | ✓ |
| sslcertdownload | ✗ | ✓ | ✓ |
| sslcertupload | ✗ | ✓ | ✓ |
| sslcertview | ✓ | ✓ | ✓ |
| sslcsrgen | ✗ | ✓ | ✓ |
| sslkeyupload | ✗ | ✓ | ✓ |
| testemail | ✓ | ✓ | ✓ |
| testtrap | ✓ | ✓ | ✓ |
| vmdisconnect | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| vmkey | ✓ | ✓ | ✓ |
| usercertupload | ✗ | ✓ | ✓ |
| usercertview | ✓ | ✓ | ✓ |
| localConRedirDisable | ✗ | ✓ | ✗ |
| ✓ = prise en charge ; ✗ = non prise en charge | | | |

---

Retour à la page du sommaire

Retour à la page du sommaire

# Présentation d'iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Integrated Dell™ Remote Access Controller6 (iDRAC6) est une solution matérielle et logicielle de gestion de systèmes fournissant des capacités de gestion à distance, la récupération de systèmes en panne et des fonctions de contrôle de l'alimentation pour les systèmes Dell PowerEdge™.

iDRAC6 utilise un microprocesseur « système sur une puce » intégré pour le système de surveillance/contrôle distant. iDRAC6 coexiste sur la carte système avec le serveur PowerEdge géré. Le système d'exploitation du serveur exécute les applications ; 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 (protocole de gestion de réseau simple) en cas d'avertissement ou d'erreur. Pour vous aider à diagnostiquer la cause probable d'une panne du système, iDRAC6 peut journaliser des données d'événement et capturer une image de l'écran lorsqu'il détecte une panne du système.

L'interface réseau iDRAC6 est activée par défaut avec l'adresse IP statique 192.168.0.120. Elle doit être configurée pour pouvoir accéder à iDRAC6. Une fois iDRAC6 configuré sur le réseau, il est accessible sur l'adresse IP qui lui a été attribuée avec l'interface Web iDRAC6, Telnet ou SSH (Secure Shell) et les protocoles de gestion de réseau pris en charge, tels que les protocoles IPMI (interface de gestion de plateforme intelligente).

---

## Fonctionnalités de gestion d'iDRAC6 Express

iDRAC6 Express fournit les fonctionnalités de gestion suivantes :

- Enregistrement de système de noms de domaine dynamique (DDNS)
- Gestion et surveillance à distance du système à distance à l'aide d'une interface Web et de la ligne de commande SM-CLP sur une connexion série, Telnet ou SSH
- Prise en charge de l'authentification Microsoft® Active Directory® : centralise les références utilisateur et les mots de passe iDRAC6 dans Active Directory à l'aide d'un schéma étendu ou d'un schéma standard
- Solution générique visant à prendre en charge l'authentification basée sur le protocole LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne requiert aucune extension de schéma sur vos services de répertoire.
- 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 de la dernière panne du système en panne 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 de Dell OpenManage IT Assistant
- Alerte iDRAC6 : vous avertit des problèmes potentiels du nud géré au moyen d'un message électronique ou d'une interruption SNMP
- Gestion de l'alimentation à distance : fournit des fonctions de gestion de l'alimentation à distance, comme l'arrêt et la réinitialisation, à partir d'une console de gestion
- Prise en charge de l'interface de gestion de plateforme intelligente (IPMI)
- Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système distant via l'interface Web
- Gestion de la sécurité au niveau du mot de passe : empêche tout accès non autorisé à un système distant
- Autorisation basée sur les rôles : permet d'attribuer des droits pour diverses tâches de gestion de systèmes
- Prise en charge IPv6 : ajoute la prise en charge IPv6, par exemple pour accéder à l'interface Web iDRAC6 à l'aide d'une adresse IPv6, spécifie l'adresse IPv6 pour le NIC iDRAC6 et spécifie un numéro de destination pour configurer une destination d'alerte SNMP IPv6.
- Prise en charge WS-MAN : assure une gestion accessible par réseau en utilisant le protocole WS-MAN (Web Services for Management).
- Prise en charge SM-CLP : ajoute la prise en charge du protocole SM-CLP (Server Management-Command Line Protocol) qui fournit des normes pour les implémentations de la CLI de gestion de systèmes.
- Restauration et récupération du micrologiciel : vous permet de démarrer à partir de l'image de micrologiciel de votre choix ou de la restaurer.

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

---

## iDRAC6 Enterprise et média VFlash

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

Le tableau 1-1 répertorie les fonctionnalités disponibles pour le contrôleur BMC, iDRAC6 Express, iDRAC6 Enterprise et le média VFlash.

**Tableau 1-1. Liste de fonctionnalités iDRAC6**

| Fonctionnalité | BMC | iDRAC6 Express | iDRAC6 Enterprise | iDRAC6 Enterprise avec VFlash |
|---|---|---|---|---|
| **Prise en charge de l'interface et des normes** | | | | |
| IPMI 2.0 | ✓ | ✓ | ✓ | ✓ |
| IUG Web | ✗ | ✓ | ✓ | ✓ |
| SNMP | ✗ | ✓ | ✓ | ✓ |
| WSMAN | ✗ | ✓ | ✓ | ✓ |
| SMASH-CLP | ✗ | ✓ | ✓ | ✓ |
| Ligne de commande RACADM | ✗ | ✗ | ✓ | ✓ |
| **Connectivité** | | | | |
| Modes réseau Partagé/Basculement | ✓ | ✓ | ✓ | ✓ |
| IPv4 | ✓ | ✓ | ✓ | ✓ |
| Marquage VLAN | ✓ | ✓ | ✓ | ✓ |
| IPv6 | ✗ | ✓ | ✓ | ✓ |
| DNS dynamique | ✗ | ✓ | ✓ | ✓ |
| NIC dédié | ✗ | ✗ | ✓ | ✓ |
| **Sécurité et authentification** | | | | |
| Autorité basée sur les rôles | ✓ | ✓ | ✓ | ✓ |
| Utilisateurs locaux | ✓ | ✓ | ✓ | ✓ |
| Service de répertoire | ✗ | ✓ | ✓ | ✓ |
| Authentification bifactorielle | ✗ | ✓ | ✓ | ✓ |
| Connexion directe | ✗ | ✓ | ✓ | ✓ |
| Cryptage SSL | ✓ | ✓ | ✓ | ✓ |
| **Gestion et conversion à distance** | | | | |
| Mise à jour de micrologiciel à distance | ✓ [1] | ✓ | ✓ | ✓ |
| Installation du système d'exploitation à distance | ✗ | ✓ | ✓ | ✓ |
| Contrôle de l'alimentation du serveur | ✓ [1] | ✓ | ✓ | ✓ |
| Série sur LAN (avec proxy) | ✓ | ✓ | ✓ | ✓ |
| Série sur LAN (sans proxy) | ✗ | ✓ | ✓ | ✓ |
| Plafonnement de l'alimentation | ✗ | ✓ | ✓ | ✓ |
| Capture de l'écran de la dernière panne | ✗ | ✓ | ✓ | ✓ |
| Capture du démarrage | ✗ | ✓ | ✓ | ✓ |
| Média virtuel | ✗ | ✗ | ✓ | ✓ |
| Console virtuelle | ✗ | ✗ | ✓ | ✓ |
| Partage de la console virtuelle | ✗ | ✗ | ✓ | ✓ |
| Disque flash virtuel | ✗ | ✗ | ✗ | ✓ |
| **Surveillance** | | | | |
| Surveillance et alertes des capteurs | ✓ [1] | ✓ | ✓ | ✓ |
| Surveillance de l'alimentation en temps réel | ✗ | ✓ | ✓ | ✓ |
| Graphique d'alimentation en temps réel | ✗ | ✓ | ✓ | ✓ |
| Compteurs d'alimentation historiques | ✗ | ✓ | ✓ | ✓ |
| **Journalisation** | | | | |

| | | | | |
|---|---|---|---|---|
| Journal des événements système (SEL) | ✓ | ✓ | ✓ | ✓ |
| Journal du RAC | ✗ | ✓ | ✓ | ✓ |
| Journal de suivi | ✗ | ✓ | ✓ | ✓ |
| Syslog distant | ✗ | ✓ | ✓ | ✓ |
| [1] : la fonctionnalité est disponible uniquement via IPMI, et non via une IUG Web | | | | |
| ✓ = pris en charge ; ✗ = non pris en charge | | | | |

iDRAC6 dispose des fonctionnalités de sécurité suivantes :

- Connexion directe, authentification bifactorielle et authentification par clé publique
- Authentification des utilisateurs via Active Directory (en option), via l'authentification LDAP (en option) ou via les références utilisateur et les mots de passe stockés sur le matériel
- Autorisation basée sur les rôles, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- Configuration des références utilisateur et des mots de passe via l'interface Web ou SM-CLP
- SM-CLP et interfaces Web, qui prennent 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.

- SSH, qui utilise une couche de transport cryptée pour une sécurité plus élevée
- Limites d'échecs d'ouverture de session par adresse IP, avec blocage de l'ouverture de session à partir de l'adresse IP lorsque la limite est dépassée
- Possibilité de limiter la plage d'adresses IP pour les clients se connectant à iDRAC6

## Plateformes prises en charge

Pour les dernières plateformes prises en charge, consultez le fichier « Lisez-moi » iDRAC6 et la *Matrice de prise en charge des logiciels des systèmes Dell* disponible à l'adresse **support.dell.com / manuals**.

## Systèmes d'exploitation pris en charge

Pour les informations les plus récentes, consultez le fichier « Lisez-moi » iDRAC6 et la *Matrice de prise en charge des logiciels des systèmes Dell* disponible à l'adresse **support.dell.com / manuals**.

## Navigateurs Web pris en charge

Pour les informations les plus récentes, consultez le fichier « Lisez-moi » iDRAC6 et la *Matrice de prise en charge des logiciels des systèmes Dell* disponible à l'adresse **support.dell.com / manuals**.

**REMARQUE :** En raison de graves défauts de sécurité, la prise en charge de SSL 2.0 a été abandonnée. Votre navigateur doit être configuré pour activer SSL 3.0 afin de fonctionner correctement.

## Connexions d'accès à distance prises en charge

Le tableau 1-2 répertorie les fonctionnalités de connexion.

**Tableau 1-2. Connexions d'accès à distance prises en charge**

| Connexion | Fonctionnalités |
|---|---|
| NIC iDRAC6 | - 10 Mbits/s/100 Mbits/s/Ethernet<br>- Prise en charge de DHCP<br>- Interruptions SNMP et notifications d'événements par e-mail<br>- Prise en charge de l'environnement de commande SM-CLP (Telnet, SSH et RACADM) pour les opérations telles que la configuration iDRAC6, le démarrage système, la réinitialisation, la mise sous tension et les commandes d'arrêt<br>- Prise en charge des utilitaires IPMI, tels que IPMItool et ipmish |

## Ports iDRAC6

Le tableau 1-3 répertorie les ports sur lesquels iDRAC6 écoute les connexions. Le tableau 1-4 identifie les ports qu'iDRAC6 utilise comme client. Ces informations sont requises pour ouvrir des pare-feu pour pouvoir accéder à distance à un iDRAC6.

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

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

**Tableau 1-4. Ports de client iDRAC6**

| Numéro de port | Fonction |
|---|---|
| 25 | SMTP |
| 53 | DNS |
| 68 | Adresse IP attribuée par DHCP |
| 69 | TFTP |
| 162 | interruption SNMP |
| 636 | LDAPS |
| 3 269 | LDAPS pour le catalogue global (CG) |

---

## Autres documents utiles

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

- L'aide en ligne iDRAC6 fournit des informations détaillées sur l'utilisation de l'interface Web.
- Le *Guide d'utilisation de Dell Lifecycle Controller* fournit des informations sur Unified Server Configurator (USC), Unified Server Configurator - Lifecycle Controller Enabled (USC - LCE) et les services distants.
- La *Matrice de prise en charge des logiciels des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- Le *Guide d'installation de Dell OpenManage Server Administrator* contient des instructions visant à vous aider à installer Dell OpenManage Server Administrator.
- Le *Guide d'installation de Dell OpenManage Management Station Software* contient des instructions visant à vous aider à installer Dell OpenManage Management Station Software qui intègre l'utilitaire de gestion de la carte mère, les outils DRAC et le snap-in d'Active Directory.
- Consultez le *Guide d'utilisation de Dell OpenManage IT Assistant* pour des informations relatives à l'utilisation d'IT Assistant.
- Pour installer un iDRAC6, consultez votre *Manuel du propriétaire du matériel*.
- Consultez le *Guide d'utilisation de Dell OpenManage Server Administrator* pour des informations sur l'installation et l'utilisation de Server Administrator.
- Consultez le *Guide d'utilisation des progiciels Dell Update Package* pour des informations sur l'obtention et l'utilisation des progiciels Dell Update Package dans le contexte de la stratégie de mise à jour de votre système.
- Consultez le *Guide d'utilisation des utilitaires du contrôleur BMC Dell OpenManage* pour des informations sur iDRAC6 et l'interface IPMI.

Les documents système suivants fournissent également 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 à la réglementation. 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 sont incluses dans le présent document ou dans un document distinct.
- Les *Instructions d'installation du rack*, fournies avec le rack, indiquent comment installer votre système dans un rack.
- Le *Guide de mise en route* présente les fonctionnalités du système, la configuration de votre système et les spécifications techniques.
- Le *Manuel du propriétaire du matériel* présente les fonctionnalités du système et contient des informations de dépannage du système et des instructions d'installation ou de remplacement des composants du système.
- La documentation relative aux logiciels de gestion de systèmes décrit les fonctionnalités, la configuration requise, l'installation et l'utilisation de base du logiciel.
- La documentation du système d'exploitation indique comment installer (au besoin), configurer et utiliser le logiciel du système d'exploitation.

- La documentation fournie avec les composants achetés séparément indique comment configurer et installer ces options.
- Des mises à jour sont parfois fournies avec le système pour décrire les modifications apportées au système, au logiciel et/ou à la documentation.

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

- Les notes de version ou les fichiers « Lisez-moi » éventuellement fournis contiennent des mises à jour de dernière minute apportées au système ou à la documentation ou bien des informations techniques avancées destinées aux utilisateurs expérimentés ou aux techniciens.

Pour plus d'informations sur les termes utilisés dans le présent document, consultez le *Glossaire* disponible sur le site Web du support de Dell à l'adresse **support.dell.com/manuals**.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Utilisation de l'interface WS-MAN

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Web Services for Management (WS-MAN) est un protocole SOAP (Simple Object Access Protocol - Protocole simple d'accès aux objets) utilisé à des fins de gestion de systèmes. WS-MAN fournit un protocole interopérable permettant aux périphériques de partager et d'échanger des données sur des réseaux. iDRAC6 utilise WS-MAN pour transmettre des informations de gestion basées sur le modèle CIM (modèle commun d'informations) de DMTF (Distributed Management Task Force) ; les informations CIM définissent les sémantiques et les types d'informations qui peuvent être manipulées au sein d'un système géré. Les interfaces de gestion de plateformes de serveurs intégrées Dell™ sont articulées autour de profils, chacun définissant les interfaces spécifiques pour un domaine de gestion ou de fonctionnalité donné. Dell a par ailleurs défini un certain nombre d'extensions de modèles et de profils qui fournissent des interfaces pour des capacités supplémentaires.

Les données disponibles par le biais de WS-MAN sont fournies par l'interface d'instrumentation iDRAC6 mappée sur les profils DMTF et profils d'extension Dell suivants :

---

## Profils CIM pris en charge

**Tableau 11-1. DMTF standard**

| DMTF standard |
|---|
| 1. Serveur de base<br>Définit les classes CIM pour la représentation du serveur hôte. |
| 2. Processeur de service :<br>Contient la définition des classes CIM pour la représentation d'iDRAC6.<br><br>**REMARQUE :** Le profil du serveur de base (ci-dessus) et le profil du processeur de service sont autonomes en ce sens que les objets qu'ils décrivent sont amalgamés avec tous les autres objets CIM définis dans les profils des composants. |
| 3. Bien physique :<br>Définit les classes CIM pour la représentation de l'aspect physique des éléments gérés. iDRAC6 utilise ce profil pour représenter les informations FRU du serveur hôte et de ses composants ainsi que la topologie physique. |
| 4. Domaine d'administration SM-CLP<br>Définit les classes CIM pour la représentation de la configuration CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP. |
| 5. Gestion de l'état de l'alimentation<br>Définit les classes CIM pour les opérations de contrôle de l'alimentation. iDRAC6 utilise ce profil pour les opérations de contrôle de l'alimentation du serveur hôte. |
| 6. Bloc d'alimentation (version 1.1)<br>Définit les classes CIM pour la représentation des blocs d'alimentation. iDRAC6 utilise ce profil pour représenter les blocs d'alimentation du serveur hôte afin de décrire la consommation énergétique, tels que les filigranes de consommation énergétique élevée ou basse. |
| 7. Service CLP<br>Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP. |
| 8. Interface IP |
| 9. Client DHCP |
| 10. Client DNS |
| 11. Port Ethernet<br>Les profils ci-dessus définissent les classes CIM pour la représentation des piles réseau. iDRAC6 utilise ces profils pour représenter la configuration du NIC iDRAC6. |
| 12. Journal des enregistrements<br>Définit les classes CIM pour la représentation de différents types de journal. iDRAC6 utilise ce profil pour représenter le journal des événements système (SEL) et le journal du RAC iDRAC6. |
| 13. Inventaire des logiciels<br>Définit les classes CIM pour faire l'inventaire des logiciels installés ou disponibles. iDRAC6 utilise ce profil pour faire l'inventaire des versions du micrologiciel iDRAC6 actuellement installées via le protocole TFTP. |
| 14. Autorisation basée sur les rôles<br>Définit les classes CIM pour la représentation des rôles. iDRAC6 utilise ce profil pour configurer les privilèges de compte iDRAC6. |

| |
|---|
| 15. Mise à jour de logiciels<br>Définit les classes CIM pour faire l'inventaire des mises à jour de logiciels disponibles. iDRAC6 utilise ce profil pour faire l'inventaire des mises à jour du micrologiciel via le protocole TFTP. |
| 16. Recueil SMASH<br>Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP. |
| 17. Enregistrement des profils<br>Définit les classes CIM pour l'annonce des implémentations des profils. iDRAC6 utilise ce profil pour annoncer ses propres profils implémentés, comme l'indique ce tableau. |
| 18. Mesures de base<br>Définit les classes CIM pour la représentation des mesures. iDRAC6 utilise ce profil pour représenter les mesures du serveur hôte afin de décrire la consommation énergétique, tels que les filigranes de consommation énergétique élevée ou basse. |
| 19. Gestion simple des identités<br>Définit les classes CIM pour la représentation des identités. iDRAC6 utilise ce profil pour configurer les comptes iDRAC6. |
| 20. Redirection USB<br>Définit les classes CIM pour la représentation de la redirection à distance des ports USB locaux. iDRAC6 utilise ce profil en concomitance avec le profil de média virtuel pour configurer le média virtuel. |
| **Extensions Dell** |
| 1. Dell™ Active Directory Client version 2.0.0<br>Définit les classes d'extension CIM et Dell pour configurer le client Active Directory iDRAC6 et les privilèges locaux pour les groupes Active Directory. |
| 2. Média virtuel Dell<br>Définit les classes d'extension CIM et Dell pour la configuration du média virtuel iDRAC6. Étend le profil de redirection USB. |
| 3. Port Ethernet Dell<br>Définit les classes d'extension CIM et Dell pour la configuration de l'interface bande latérale NIC pour le NIC iDRAC6. Étend le profil du port Ethernet. |
| 4. Gestion de l'utilisation de l'alimentation Dell<br>Définit les classes d'extension CIM et Dell pour la représentation du bilan de puissance du serveur hôte et pour la configuration/surveillance du bilan de puissance du serveur hôte. |
| 5. Déploiement du SE Dell<br>Définit les classes d'extension CIM et Dell pour la représentation de la configuration des fonctionnalités de déploiement du SE. Il étend les capacités de gestion des profils de référencement en ajoutant la capacité de prise en charge des activités de déploiement du SE en manipulant les fonctionnalités de déploiement du SE offertes par le processeur de service. |

L'implémentation WS-MAN iDRAC6 utilise SSL sur le port 443 pour la sécurité du transport et prend en charge l'authentification de base et Digest. Les interfaces de services Web peuvent être utilisées en exploitant l'infrastructure client comme Windows® WinRM et la CLI Powershell, les utilitaires Open Source comme WSMANCLI et les environnements de programmation d'applications comme Microsoft® .NET®.

Des guides d'implémentation, des livres blancs, des profils et des exemples de codes supplémentaires sont disponibles dans le centre Dell Enterprise Technology Center à l'adresse **www.delltechcenter.com**. Pour plus d'informations, consultez également :

- Le site Web DTMF : **www.dmtf.org/standards/profiles/**
- Les notes de diffusion ou le fichier « Lisez-moi » de WS-MAN.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Utilisation de l'interface de ligne de commande SM-CLP iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Cette section fournit des informations sur le protocole Server Management-Command Line Protocol (SM-CLP) de Distributed Management Task Force (DMTF) qui est incorporé dans iDRAC6.

**REMARQUE :** Cette section suppose que vous connaissez l'initiative SMASH (Systems Management Architecture for Server Hardware) et les spécifications SM-CLP. Pour plus d'informations sur ces spécifications, consultez le site Web de DMTF à l'adresse **www.dmtf.org**.

SM-CLP iDRAC6 est un protocole qui fournit des normes aux implémentations de la CLI de gestion de systèmes. SM-CLP est un sous-composant de l'initiative SMASH DMTF destinée à rationaliser la gestion de serveur sur des plateformes multiples. La spécification SM-CLP, conjointement à Managed Element Addressing Specification et à de nombreux profils de spécifications de mappage SM-CLP, décrit les verbes et les cibles normalisés pour les diverses exécutions de tâches de gestion.

---

## Prise en charge de SM-CLP iDRAC6

SM-CLP est hébergé par le micrologiciel du contrôleur iDRAC6 et prend en charge les interfaces Telnet, SSH et série. L'interface SM-CLP iDRAC6 est basée sur la spécification SM-CLP, version 1.0, fournie par l'organisation DMTF. SM-CLP iDRAC6 prend en charge tous les profils décrits dans le tableau 11-1 « Profils CIM pris en charge ».

Les sections suivantes fournissent un aperçu de la fonctionnalité SM-CLP qui est hébergée par iDRAC6.

---

## Fonctionnalités de SM-CLP

SM-CLP encourage la conception de verbes et de cibles pour fournir des capacités de gestion de systèmes via la CLI. Le verbe indique l'opération à effectuer et la cible détermine l'entité (ou l'objet) qui exécute l'opération.

Voici un exemple de la syntaxe de ligne de commande de SM-CLP.

```
<verbe> [<options>] [<cible>] [<propriétés>]
```

Pendant une session SM-CLP type, vous pouvez effectuer des opérations à l'aide des verbes énumérés dans le tableau 12-1.

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

| Verbe | Définition |
|---|---|
| cd | Navigue dans MAP à l'aide de l'environnement |
| set | Définit une propriété sur une valeur spécifique |
| help | Affiche l'aide pour une cible spécifique |
| reset | Réinitialise la cible |
| show | Affiche les propriétés, les verbes et les sous-cibles de la cible |
| start | Active une cible |
| stop | Arrête une cible |
| exit | Quitte la session d'environnement SM-CLP |
| version | Affiche les attributs de version d'une cible |
| load | Déplace une image binaire d'une URL vers une adresse cible spécifiée |

## Utilisation de SM-CLP

SSH (ou Telnet) vers iDRAC6 avec les bonnes références.

L'invite SMCLP (/admin1->) est affichée.

## Cibles SM-CLP

Le tableau 12-2 donne une liste des cibles fournies par SM-CLP pour prendre en charge les opérations décrites dans le tableau 12-1 ci-dessus.

**Tableau 12-2. Cibles SM-CLP**

| | |
|---|---|

| Cible | Définitions |
|---|---|
| admin1 | domaine admin |
| admin1/profiles1 | Profils enregistrés dans iDRAC6 |
| admin1/hdwr1 | Matériel |
| admin1/system1 | Cible du système géré |
| admin1/system1/redundancyset1 | Bloc d'alimentation |
| admin1/system1/redundancyset1/pwrsupply* | Bloc d'alimentation du système géré |
| admin1/system1/sensors1 | Détecteurs du système géré |
| admin1/system1/capabilities1 | Capacités de recueil SMASH du système géré |
| admin1/system1/capabilities1/ pwrcap1 | Capacités d'utilisation de l'alimentation du système géré |
| admin1/system1/capabilities1/ elecap1 | Capacités de cible du système géré |
| admin1/system1/logs1 | Cible des recueils du journal des enregistrements |
| admin1/system1/logs1/log1 | Entrée d'enregistrement du journal d'événements système (SEL) |
| admin1/system1/logs1/log1/ record* | Instance d'enregistrement SEL individuelle sur le système géré |
| admin1/system1/settings1 | Paramètres de recueil SMASH du système géré |
| admin1/system1/settings1/ pwrmaxsetting1 | Paramètre d'allocation de puissance maximale du système géré |
| admin1/system1/settings1/ pwrminsetting1 | Paramètre d'allocation de puissance minimale du système géré |
| admin1/system1/capacities1 | Recueil SMASH des capacités du système géré |
| admin1/system1/consoles1 | Recueil SMASH des consoles du système géré |
| admin1/system1/usbredirectsap1 | SAP de redirection USB du média virtuel |
| admin1/system1/usbredirectsap1/remotesap1 | SAP de redirection USB de destination du média virtuel |
| admin1/system1/sp1 | Processeur de service |
| admin1/system1/sp1/timesvc1 | Service de temps du processeur de service |
| admin1/system1/sp1/capabilities1 | Recueil SMASH des capacités du processeur de service |
| admin1/system1/sp1/capabilities1/clpcap1 | Capacités de service CLP |
| admin1/system1/sp1/capabilities1/pwrmgtcap1 | Capacités de service de gestion de l'état de l'alimentation sur le système |
| admin1/system1/sp1/capabilities1/ipcap1 | Capacités d'interface IP |
| admin1/system1/sp1/capabilities1/dhcpcap1 | Capacités de client DHCP |
| admin1/system1/sp1/capabilities1/NetPortCfgcap1 | Capacités de configuration de port réseau |
| admin1/system1/sp1/capabilities1/usbredirectcap1 | SAP de redirection USB des capacités de média virtuel |
| admin1/system1/sp1/capabilities1/vmsapcap1 | Capacités SAP de média virtuel |
| admin1/system1/sp1/capabilities1/swinstallsvccap1 | Capacités de service d'installation de logiciel |
| admin1/system1/sp1/capabilities1/acctmgtcap* | Capacités de service de gestion de comptes |
| admin1/system1/sp1/capabilities1/adcap1 | Capacités Active Directory |
| admin1/system1/sp1/capabilities1/rolemgtcap* | Capacités de gestion basée sur les rôles locaux |
| admin1/system1/sp1/capabilities/PwrutilmgtCap1 | Capacités de gestion de l'utilisation de l'alimentation |
| admin1/system1/sp1/capabilities/metriccap1 | Capacités de service de mesure |
| admin1/system1/sp1/capabilities1/elecap1 | Capacités d'authentification multifacteurs |
| admin1/system1/sp1/capabilities1/lanendptcap1 | Capacités de terminaison LAN (port Ethernet) |
| admin1/system1/sp1/logs1 | Recueil des journaux du processeur de service |
| admin1/system1/sp1/logs1/log1 | Journal des enregistrements système |
| admin1/system1/sp1/logs1/log1/record* | Entrée du journal système |
| admin1/system1/sp1/settings1 | Recueil des paramètres du processeur de service |
| admin1/system1/sp1/settings1/ clpsetting1 | Données des paramètres de service CLP |
| admin1/system1/sp1/settings1/ ipsettings1 | Données des paramètres d'affectation d'interface IP (statique) |
| admin1/system1/sp1/settings1/ ipsettings1/staticipsettings1 | Données des paramètres d'affectation d'interface IP statique |
| admin1/system1/sp1/settings1/ ipsettings1/dnssettings1 | Données des paramètres du client DNS |
| admin1/system1/sp1/settings1/ ipsettings2 | Données des paramètres d'affectation d'interface IP (DHCP) |
| admin1/system1/sp1/settings1/ ipsettings2/dhcpsettings1 | Données des paramètres du client DHCP |
| admin1/system1/sp1/clpsvc1 | Service de protocole de service CLP |
| admin1/system1/sp1/clpsvc1/ clpendpt* | Terminaison de protocole de service CLP |

| | |
|---|---|
| admin1/system1/sp1/clpsvc1/<br>tcpendpt* | Terminaison TCP de protocole de service CLP |
| admin1/system1/sp1/jobq1 | File d'attente de tâches de protocole de service CLP |
| admin1/system1/sp1/jobq1/job* | Tâche de protocole de service CLP |
| admin1/system1/sp1/pwrmgtsvc1 | Service de gestion de l'état de l'alimentation |
| admin1/system1/sp1/ipcfgsvc1 | Service de configuration d'interface IP |
| admin1/system1/sp1/ipendpt1 | Terminaison de protocole d'interface IP |
| admin1/system1/sp1/<br>ipendpt1/gateway1 | Passerelle d'interface IP |
| admin1/system1/sp1/<br>ipendpt1/dhcpendpt1 | Terminaison de protocole de client DHCP |
| admin1/system1/sp1/<br>ipendpt1/dnsendpt1 | Terminaison de protocole de client DNS |
| admin1/system1/sp1/ipendpt1/<br>dnsendpt1/dnsserver* | Serveur client DNS |
| admin1/system1/sp1/NetPortCfgsvc1 | Service de configuration de port réseau |
| admin1/system1/sp1/lanendpt1 | Terminaison LAN |
| admin1/system1/sp1/<br>lanendpt1/enetport1 | Port Ethernet |
| admin1/system1/sp1/VMediaSvc1 | Service de média virtuel |
| admin1/system1/sp1/<br>VMediaSvc1/tcpendpt1 | Terminaison de protocole TCP de média virtuel |
| admin1/system1/sp1/swid1 | Identité de logiciel |
| admin1/system1/sp1/<br>swinstallsvc1 | Service d'installation de logiciel |
| admin1/system1/sp1/<br>account1-16 | Compte d'authentification multifacteurs (MFA) |
| admin1/sysetm1/sp1/<br>account1-16/identity1 | Compte d'identité d'utilisateur local |
| admin1/sysetm1/sp1/<br>account1-16/identity2 | Compte d'identité IPMI (LAN) |
| admin1/sysetm1/sp1/<br>account1-16/identity3 | Compte d'identité IPMI (série) |
| admin1/sysetm1/sp1/<br>account1-16/identity4 | Compte d'identité CLP |
| admin1/system1/sp1/acctsvc1 | Service de gestion de compte MFA |
| admin1/system1/sp1/acctsvc2 | Service de gestion de compte IPMI |
| admin1/system1/sp1/acctsvc3 | Service de gestion de compte CLP |
| admin1/system1/sp1/group1-5 | Groupe Active Directory |
| admin1/system1/sp1/<br>group1-5/identity1 | Identité Active Directory |
| admin1/system1/sp1/ADSvc1 | Service Active Directory |
| admin1/system1/sp1/rolesvc1 | Service d'autorisation basée sur les rôles (RBA) locaux |
| admin1/system1/sp1/rolesvc1/<br>Role1-16 | Rôle local |
| admin1/system1/sp1/rolesvc1/<br>Role1-16/privilege1 | Privilège de rôle local |
| admin1/system1/sp1/rolesvc1/<br>Role17-21/ | Rôle Active Directory |
| admin1/system1/sp1/rolesvc1/<br>Role17-21/privilege1 | Privilège Active Directory |
| admin1/system1/sp1/rolesvc2 | Service RBA IPMI |
| admin1/system1/sp1/rolesvc2/<br>Role1-3 | Rôle IPMI |
| admin1/system1/sp1/rolesvc2/<br>Role4 | Rôle série sur LAN (SOL) IPMI |
| admin1/system1/sp1/rolesvc3 | Service RBA CLP |
| admin1/system1/sp1/rolesvc3/<br>Role1-3 | Rôle CLP |
| admin1/system1/sp1/rolesvc3/<br>Role1-3/privilege1 | Privilège de rôle CLP |
| admin1/system1/sp1/<br>pwrutilmgtsvc1 | Service de gestion de l'utilisation de l'alimentation |
| admin1/system1/sp1/<br>pwrutilmgtsvc1/pwrcurr1 | Données des paramètres d'allocation de l'alimentation actuelle du service de gestion de l'utilisation de l'alimentation |
| admin1/system1/sp1/metricsvc1 | Service de mesure |
| admin1/system1/sp1/metricsvc1/cumbmd1 | Définition de la mesure de base cumulée |
| /admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1 | Valeur de la mesure de base cumulée |
| /admin1/system1/sp1/metricsvc1/cumwattamd1 | Définition de la mesure de l'agrégation de la puissance cumulée en watts |

| | |
|---|---|
| /admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1 | Valeur de la mesure de l'agrégation de la puissance cumulée en watts |
| /admin1/system1/sp1/metricsvc1/cumampamd1 | Définition de la mesure de l'agrégation de la puissance cumulée en ampères |
| /admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1 | Valeur de la mesure de l'agrégation de la puissance cumulée en ampères |
| /admin1/system1/sp1/metricsvc1/loamd1 | Définition de la mesure de l'agrégation de la consommation basse |
| /admin1/system1/sp1/metricsvc1/loamd1/loamv* | Valeur de la mesure de l'agrégation de la consommation basse |
| /admin1/system1/sp1/metricsvc1/hiamd1 | Définition de la mesure de l'agrégation de la consommation élevée |
| /admin1/system1/sp1/metricsvc1/hiamd1/hiamv* | Valeur de la mesure de l'agrégation de la consommation élevée |
| /admin1/system1/sp1/metricsvc1/avgamd1 | Définition de la mesure de l'agrégation de la consommation moyenne |
| /admin1/system1/sp1/metricsvc1/avgamd1/avgamv* | Valeur de la mesure de l'agrégation de la consommation moyenne |

Retour à la page du sommaire

Retour à la page du sommaire

# Déploiement de votre système d'exploitation en utilisant VMCLI

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



L'utilitaire d'interface de ligne de commande de média virtuel (VMCLI) est une interface de ligne de commande qui fournit les fonctionnalités de média virtuel de la station de gestion à iDRAC6 dans le système distant. À l'aide de VMCLI et de méthodes avec script, vous pouvez déployer votre système d'exploitation sur plusieurs systèmes distants au sein de votre réseau.

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

---

## Avant de commencer

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

### Exigences du système distant

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 test à l'aide de l'interface utilisateur Web iDRAC6, puis redémarrez le système.

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

### Création d'un fichier image pour les systèmes Linux

Utilisez l'utilitaire de duplicateur de données (dd) pour créer un fichier image de démarrage pour votre système Linux.

Pour exécuter l'utilitaire, ouvrez une invite de commande et tapez les commandes suivantes :

```
dd if=<périphérique-d'entrée> of=<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. Incluez les programmes et/ou les scripts utilisés pour les procédures de déploiement de système d'exploitation.

   Par exemple, pour déployer un système d'exploitation Windows, le fichier image peut inclure des programmes qui sont semblables aux méthodes de déploiement utilisées par Microsoft Systems Management Server (SMS).

   Lorsque vous créez le fichier image, procédez comme suit :

   - Suivez les procédures d'installation réseau standard
   - Marquez l'image de déploiement en *lecture seule* pour garantir que chaque système cible démarre et exécute la même procédure de déploiement
4. Effectuez l'une des procédures suivantes :

- Intégrez **IPMItool** et VMCLI dans votre application de déploiement de système d'exploitation existante. Utilisez l'exemple de script **vm6deploy** comme guide d'utilisation de l'utilitaire.
- Utilisez le script **vm6deploy** existant pour déployer votre système d'exploitation.

---

# Déploiement du système d'exploitation

Utilisez l'utilitaire VMCLI et le script **vm6deploy** inclus avec l'utilitaire pour déployer le système d'exploitation sur vos systèmes distants.

Avant de commencer, vérifiez l'exemple de script **vm6deploy** inclus avec l'utilitaire VMCLI. Le script affiche les étapes détaillées requises pour déployer le système d'exploitation sur les systèmes distants de votre réseau.

La procédure suivante fournit un aperçu de haut niveau du déploiement du système d'exploitation sur les systèmes distants ciblés.

1. Répertoriez les adresses IPv4 ou IPv6 iDRAC6 des systèmes distants qui seront déployées dans le fichier texte **ip.txt**, en indiquant une seule adresse IPv4 ou IPv6 par ligne.
2. Insérez un CD ou un DVD de système d'exploitation de démarrage dans le lecteur de média client.
3. Exécutez **vm6deploy** à la ligne de commande.

Pour exécuter le script **vm6deploy**, saisissez la commande suivante à l'invite de commande :

```
vm6deploy -r ip.txt -u <utilisateur-idrac> -p <mot-de-passe-utilisateur-idrac> -c {<image-iso9660> | <chemin>} -f {<lecteur-de-disquette> ou
<image-de-disquette>}
```

où :

- <*utilisateur-idrac*> est le nom d'utilisateur iDRAC6, par exemple **root**
- <*mot-de-passe-utilisateur-idrac*> est le mot de passe de l'utilisateur iDRAC6, par exemple **calvin**
- <*image-iso9660*> est le chemin d'une image ISO9660 du CD ou du DVD d'installation du système d'exploitation
- -f {<*lecteur-de-disquette*>} est le chemin du périphérique contenant le CD, le DVD ou la disquette d'installation du système d'exploitation
- <*image-de-disquette*> est le chemin d'une image de disquette valide

Le script **vm6deploy** transmet ses options de ligne de commande à l'utilitaire **VMCLI**. Consultez « Options de ligne de commande » pour obtenir des détails sur ces options. Le script traite l'option **-r** de manière légèrement différente de l'option **vmcli -r**. Si l'argument de l'option **-r** est le nom d'un fichier existant, le script lit les adresses IPv4 ou IPv6 iDRAC6 du fichier spécifié et exécute l'utilitaire **VMCLI** une fois pour chaque ligne. Si l'argument de l'option **-r** n'est pas un nom de fichier, il doit correspondre à l'adresse d'un iDRAC6 unique. Dans ce cas, l'option **-r** fonctionne comme décrit pour l'utilitaire **VMCLI**.

---

# Utilisation de l'utilitaire VMCLI

L'utilitaire VMCLI est une interface de ligne de commande scriptable qui fournit les fonctionnalités de média virtuel de la station de gestion à iDRAC6.

L'utilitaire VMCLI fournit les fonctionnalités suivantes :

**REMARQUE :** Lors de la virtualisation de fichiers image en lecture seule, plusieurs sessions peuvent partager le même média image. Lors de la virtualisation de lecteurs physiques, une seule 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 Secure Sockets Layer (SSL)

Avant d'exécuter l'utilitaire, assurez-vous que vous disposez des privilèges utilisateur de média virtuel pour iDRAC6.

**PRÉCAUTION : Il est recommandé d'utiliser l'option '-i' d'indicateur interactif au démarrage de l'utilitaire de la ligne de commande VMCLI. Ceci permet de garantir une sécurité plus poussée en préservant la confidentialité du nom d'utilisateur et du mot de passe, car sur de nombreux systèmes d'exploitation Windows et Linux, le nom d'utilisateur et le mot de passe sont visibles lorsque les processus sont examinés par d'autres utilisateurs.**

Si votre système d'exploitation prend en charge des privilèges Administrateur ou un privilège spécifique au système d'exploitation ou une appartenance au groupe, les privilèges Administrateur sont également requis pour exécuter la commande VMCLI.

L'administrateur du système client contrôle les groupes et les privilèges d'utilisateurs, contrôlant ainsi les utilisateurs qui peuvent exécuter l'utilitaire.

Pour les systèmes Windows, vous devez disposer des privilèges Utilisateur privilégié pour pouvoir exécuter l'utilitaire VMCLI.

Pour les systèmes Linux, vous pouvez accéder à l'utilitaire VMCLI sans privilèges Administrateur en utilisant la commande **sudo**. Cette commande offre un moyen centralisé de fournir un accès non-administrateur et permet de journaliser toutes les commandes d'utilisateur. Pour ajouter ou modifier des utilisateurs dans le groupe VMCLI, l'administrateur utilise la commande **visudo**. Les utilisateurs sans privilèges Administrateur peuvent ajouter la commande **sudo** comme préfixe à la ligne de commande VMCLI (ou au script VMCLI) afin d'accéder à iDRAC6 dans le système distant et d'exécuter l'utilitaire.

## Installation de l'utilitaire VMCLI

L'utilitaire VMCLI se trouve sur le DVD *Dell Systems Management Tools and Documentation* qui est inclus avec votre kit Dell™ OpenManage™ Systems Management Software. Pour installer l'utilitaire, insérez le DVD *Dell Systems Management Tools and Documentation* dans le lecteur de DVD de votre système et suivez les instructions qui s'affichent à l'écran.

Le DVD *Dell Systems Management Tools and Documentation* contient les derniers produits Systems Management Software, notamment la gestion du stockage, le service d'accès à distance et l'utilitaire IPMItool. Ce DVD contient également des fichiers « Lisez-moi », qui fournissent les dernières informations sur les produits Systems Management Software.

Le DVD *Dell Systems Management Tools and Documentation* inclut **vm6deploy**, un exemple de script qui illustre l'utilisation des utilitaires VMCLI et IPMItool pour déployer le logiciel sur plusieurs systèmes distants.

**REMARQUE :** Le script **vm6deploy** dépend des autres fichiers présents dans son répertoire lors de son installation. Si vous souhaitez utiliser le script à partir d'un autre répertoire, vous devez copier tous les fichiers avec ce script. Si l'utilitaire IPMItool n'est pas installé, l'utilitaire doit être copié en plus des autres fichiers.

## Options de ligne de commande

L'interface VMCLI est identique sur les systèmes Windows et Linux.

Le format d'une commande VMCLI est comme suit :

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

La syntaxe de ligne de commande est sensible à la casse. Pour plus d'informations, consultez « Paramètres VMCLI ».

Si le système distant accepte les commandes et si iDRAC6 autorise la connexion, la commande continue de s'exécuter jusqu'à ce qu'un des événements suivants se produise :

- La connexion VMCLI est interrompue pour une raison quelconque.
- Le processus est manuellement interrompu à l'aide d'une commande de système d'exploitation. Par exemple, sous Windows, vous pouvez utiliser le gestionnaire des tâches pour interrompre le processus.

## Paramètres VMCLI

### Adresse IP iDRAC6

*`-r <adresse-IP-iDRAC[:port-SSL-iDRAC]>`*

Ce paramètre fournit l'adresse IPv4 ou IPv6 iDRAC6 et le port SSL, dont l'utilitaire a besoin pour établir une connexion de média virtuel avec l'iDRAC6 cible. Si vous saisissez une adresse IPv4 ou IPv6 ou un nom DDNS non valide, un message d'erreur s'affiche et la commande se termine.

*<adresse-IP-iDRAC>* est une adresse IPv4 ou IPv6 unique valide ou le nom DDNS (Dynamic Domain Naming System) iDRAC6 (s'il est pris en charge). Si *<port-SSL-iDRAC>* est omis, le port 443 (port par défaut) est utilisé. Le port SSL optionnel n'est pas obligatoire à moins que vous ne modifiez le port SSL par défaut iDRAC6.

## Nom d'utilisateur iDRAC6

`-u <utilisateur-iDRAC>`

Ce paramètre fournit le nom d'utilisateur iDRAC6 qui exécutera le média virtuel.

*<utilisateur-iDRAC>* doit avoir les attributs suivants :

- Nom d'utilisateur valide
- Droit 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 {<périphérique-de-disquette> ou <image-de-disquette>} et/ou`

`-c {<périphérique-CD-DVD> ou <image-de-CD-DVD>}`

où <périphérique-de-disquette> ou <périphérique-de-CD-DVD> est une lettre de lecteur valide (pour les systèmes Windows) ou un nom de fichier de périphérique valide (pour les systèmes Linux), et <image-de-disquette> ou <image-de-CD-DVD> est le nom de fichier et le chemin d'un fichier image valide.

**REMARQUE :** Les points de montage ne sont pas pris en charge pour l'utilitaire VMCLI.

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

Par exemple, un fichier image est spécifié comme :

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

`-f/tmp/myfloppy.img` (système Linux)

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

Par exemple, un périphérique est spécifié comme :

`-f a:\` (système Windows)

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

**REMARQUE :** Red Hat® Enterprise Linux® version 4 ne prend pas en charge les LUN multiples. Toutefois, le noyau prend en charge cette fonctionnalité. Permettez à Red Hat Enterprise Linux version 4 de reconnaître un périphérique SCSI doté de LUN multiples en procédant comme suit :

1. Modifiez **/etc/modprobe.conf** et ajoutez la ligne suivante :
   options scsi_mod max_luns=8
   (Vous pouvez spécifier 8 LUN ou n'importe quel nombre supérieur à 1.)

2. Récupérez le nom de l'image de kernel en tapant la commande suivante à la ligne de commande :

   uname -r

3. Allez dans le répertoire **/boot** et supprimez le fichier image de kernel dont vous avez déterminé le nom à l'étape 2 :

   mkinitrd /boot/initrd-'uname -r'.img `uname -r'

4. Redémarrez le serveur.

5. Exécutez la commande suivante pour confirmer que la prise en charge de LUN multiples a été ajoutée pour le nombre de LUN spécifié à l'étape 1 :

   cat /sys/modules/scsi_mod/max_luns

Si le périphérique fournit une capacité de protection contre l'écriture, utilisez-la pour garantir que le média virtuel n'écrira pas sur le média.

Omettez ce paramètre de la ligne de commande si vous ne virtualisez pas le média de disquette. Si une valeur non valide est détectée, un message d'erreur s'affiche et la commande se termine.

### Périphérique ou fichier image de CD/DVD

`-c {<nom-de-périphérique> | <fichier-image>}`

où <*nom-de-périphérique*> est une lettre de lecteur de CD/DVD valide (systèmes Windows) ou un nom de fichier de périphérique de CD/DVD valide (systèmes Linux), et <*fichier-image*> est le nom de fichier et le chemin d'un fichier image ISO-9660 valide.

Ce paramètre spécifie le périphérique ou le fichier qui fournira le média de CD/DVD-ROM virtuel :

Par exemple, un fichier image est spécifié comme :

`-c c:\temp\mydvd.img` (systèmes Windows)

`-c/tmp/mydvd.img` (systèmes Linux)

Par exemple, un périphérique est spécifié comme :

`-c d:\` (systèmes Microsoft® Windows®)

`-c/dev/cdrom` (systèmes Linux)

Omettez ce paramètre de la ligne de commande si vous ne virtualisez pas le média de CD/DVD. Si une valeur non valide est détectée, un message d'erreur s'affiche et la commande se termine.

Spécifiez au moins un type de média (lecteur de disquette ou de CD/DVD) avec la commande, à moins que seules des options de commutateur ne soient fournies. Sinon, un message d'erreur s'affiche et la commande se termine en générant une erreur.

### Affichage de la version

`-v`

Ce paramètre est utilisé pour afficher la version de l'utilitaire VMCLI. Si aucune autre option de non-commutateur n'est fournie, la commande est interrompue sans message d'erreur.

### Affichage de l'aide

`-h`

Ce paramètre permet d'afficher un résumé des paramètres de l'utilitaire VMCLI. Si aucune autre option de non-commutateur n'est fournie, la commande est interrompue sans erreur.

### Données cryptées

`-e`

Lorsque ce paramètre est inclus dans la ligne de commande, VMCLI utilise un *canal crypté SSL* pour transférer des données entre la station de gestion et iDRAC6 dans le système distant. Si ce paramètre n'est pas inclus dans la ligne de commande, le transfert de données n'est pas crypté.

**REMARQUE :** L'utilisation de cette option ne modifie pas l'état affiché du cryptage de média virtuel sur *activé* dans les autres interfaces de configuration iDRAC6 comme RACADM ou l'interface Web.

## Options d'environnement de système d'exploitation VMCLI

Les fonctionnalités de système d'exploitation suivantes peuvent être utilisées sur la ligne de commande VMCLI :

- stderr/stdout redirection : redirige la sortie imprimée de l'utilitaire vers un fichier.

  Par exemple, le caractère plus grand que (>), suivi par un nom de fichier, écrase le fichier indiqué avec la sortie imprimée de l'utilitaire VMCLI.

  **REMARQUE :** L'utilitaire VMCLI ne lit pas à partir d'une entrée standard (**stdin**). Par conséquent, la redirection **stdin** n'est pas exigée.

- Exécution en arrière-plan : par défaut, l'utilitaire VMCLI s'exécute en avant-plan. Utilisez les fonctionnalités d'environnement de la commande du système d'exploitation pour exécuter l'utilitaire en arrière-plan. Par exemple, dans un système d'exploitation Linux, le caractère d'esperluette (&) qui suit la commande fait que le programme est engendré comme un nouveau processus en arrière-plan.

La dernière technique est utile dans les programmes de script, car elle permet au script de se poursuivre après le démarrage d'un nouveau processus pour la commande VMCLI (sinon, le script serait bloqué jusqu'à ce que le programme VMCLI soit terminé). Lorsque plusieurs instances VMCLI sont démarrées de cette manière et qu'une ou plusieurs instances de commande doivent être terminées manuellement, utilisez les fonctionnalités spécifiques au système d'exploitation pour répertorier et terminer les processus.

### Codes de retour VMCLI

Les messages de texte en anglais seulement sont émis vers la sortie d'erreur standard chaque fois que des erreurs sont rencontrées.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration de l'interface de gestion de plateforme intelligente (IPMI)

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



---

## Configuration d'IPMI

Cette section fournit des informations sur la configuration et l'utilisation de l'interface IPMI iDRAC6. L'interface comprend :

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

iDRAC6 est compatible IPMI 2.0. Vous pouvez configurer IPMI iDRAC6 en utilisant :

- l'IUG iDRAC6 depuis votre navigateur,
- un utilitaire Open Source comme *IPMItool*,
- l'environnement IPMI Dell™ OpenManage™ : *ipmish*
- RACADM.

Pour plus d'informations sur l'utilisation de l'environnement IPMI, ipmish, consultez le Guide d'utilisation de *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com / manuals**.

Pour plus d'informations sur l'utilisation de la RACADM, consultez « Utilisation de la RACADM à distance ».

### Configuration d'IPMI à l'aide de l'interface Web

Pour des informations détaillées, consultez « Configuration d'IPMI ».

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

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

2. Configurez IPMI sur LAN.

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

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

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

   a. Mettez à jour les privilèges du canal IPMI.

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

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

      où <*niveau*> correspond à :

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

      Par exemple, pour définir le privilège Canal LAN IPMI sur 2 (utilisateur), tapez la commande suivante :

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

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

   **REMARQUE :** IPMI iDRAC6 prend en charge le protocole RMCP+. Pour plus d'informations, consultez les spécifications d'IPMI 2.0.

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

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

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

3. Configurez les communications série IPMI sur LAN (SOL).

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

   racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1

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

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

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

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

   où *<niveau>* correspond à :

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

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

   racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2

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

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

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

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

   où *<débit_en_bauds>* est égal à 9 600, 19 200, 57 600 ou 115 200 b/s.

   Par exemple :

   racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600

   c. Activez SOL pour un utilisateur individuel.

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

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

   racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i *<référence>* 2

   où *<référence>* est la référence unique de l'utilisateur.

4. Configurez les communications IPMI série.

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

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

   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0

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

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

   racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate *<débit_en_bauds>*

   où *<débit_en_bauds>* est égal à 9 600, 19 200, 57 600 ou 115 200 b/s.

   Par exemple :

   racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600

   c. Activez le contrôle du débit matériel des communications IPMI série.

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

   racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1

d. Configurez le niveau de privilège minimal de canal des communications IPMI série.

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

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

   où <*niveau*> correspond à :

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

   Par exemple, pour définir les privilèges de canal des communications IPMI série sur 2 (utilisateur), tapez la commande suivante :

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
   ```

e. Assurez-vous que MUX série est correctement configuré dans le programme de configuration du BIOS.

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

   La configuration IPMI est terminée.

   Si les communications IPMI série sont en mode terminal, vous pouvez configurer les paramètres supplémentaires suivants à l'aide des commandes **racadm config cfgIpmiSerial :**

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

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

## Utilisation de l'interface série d'accès à distance IPMI

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

- **Mode terminal IPMI :** prend en charge les commandes ASCII qui sont envoyées à partir d'un terminal série. Le jeu de commandes a un nombre limité de commandes (notamment le contrôle de l'alimentation) et prend en charge les commandes IPMI brutes qui sont saisies sous forme de caractères ASCII hexadécimaux.
- **Mode de base IPMI :** prend en charge une interface binaire pour l'accès au programme, comme l'environnement IPMI (IPMISH) qui est inclus avec l'utilitaire de gestion de la carte mère (BMU).

Pour configurer le mode IPMI à l'aide de la RACADM :

1. Désactivez l'interface série du RAC.

   À l'invite de commande, tapez :

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

2. Activez le mode IPMI approprié.

   Par exemple, à l'invite de commande, tapez :

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 ou 1>
   ```

Pour plus d'informations, consultez « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

---

# Configuration des communications série sur LAN au moyen de l'interface Web

Pour des informations détaillées, consultez « Configuration d'IPMI ».

**REMARQUE :** Vous pouvez utiliser les communications série sur LAN avec les outils Dell OpenManage suivants : SOLProxy et IPMItool. Pour plus d'informations, consultez le Guide d'utilisation de *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com / manuals**.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration et utilisation du média virtuel

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**

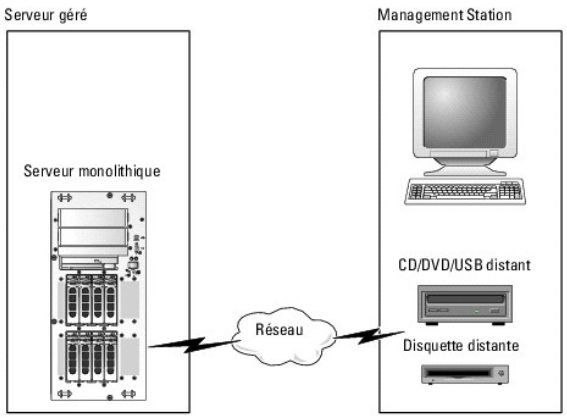


---

## Présentation

La fonctionnalité **Média virtuel**, accessible via le visualiseur de redirection de console, permet au serveur géré d'accéder au média connecté à un système distant sur le réseau. La figure 15-1 illustre l'architecture globale d'un **média virtuel**.

**Figure 15-1. Architecture globale d'un média virtuel**




Grâce au **média virtuel**, les administrateurs peuvent démarrer à distance leurs serveurs gérés, installer des applications, mettre à jour des pilotes ou même installer de nouveaux systèmes d'exploitation à distance à partir de lecteurs de CD/DVD et de disquettes virtuels.

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

Le **média virtuel** définit deux périphériques pour le système d'exploitation et le BIOS du serveur géré : un périphérique de disquette et un périphérique de disque optique.

La station de gestion fournit le média physique ou le fichier image sur le réseau. Lorsque le **média virtuel** est connecté ou autoconnecté, toutes les requêtes d'accès au lecteur de CD/disquette virtuel provenant du serveur géré sont dirigées vers la station de gestion par le réseau. La connexion du **média virtuel** revient à insérer le média dans des périphériques physiques sur le système géré. Lorsque le **média virtuel** se trouve dans l'état de connexion, les périphériques virtuels du système géré se présentent sous la forme de deux lecteurs sur lesquels le média n'est pas installé.

Le tableau 15-1 répertorie les connexions de lecteur prises en charge pour les lecteurs de disquette virtuels et les lecteurs optiques virtuels.

**REMARQUE :** Le changement de **média virtuel** en cours de connexion est susceptible d'interrompre la séquence de démarrage du système.

**Tableau 15-1. Connexions de lecteur prises en charge**

| Connexions de lecteur de disquette virtuel prises en charge | Connexions de lecteur optique virtuel prises en charge |
|---|---|
| Lecteur de disquette 1.44 hérité avec disquette 1.44 | Lecteur de CD-ROM, de DVD, CD-RW, mixte avec média de CD-ROM |
| Lecteur de disquette USB avec disquette 1.44 | Fichier image de CD-ROM/DVD au format ISO9660 |
| Image de disquette 1.44 | Lecteur de CD-ROM USB avec média de CD-ROM |
| Disque amovible USB | |

### Station de gestion Windows

Pour exécuter la fonctionnalité **Média virtuel** sur une station de gestion exécutant le système d'exploitation Microsoft® Windows®, installez une version prise en charge d'Internet Explorer ou de Firefox avec un environnement d'exécution Java (JRE).

### Station de gestion Linux

Pour exécuter la fonctionnalité Média virtuel sur une station de gestion exécutant le système d'exploitation Linux, installez une version prise en charge de Firefox.

Un environnement d'exécution Java (JRE) 32 bits est requis pour exécuter le plug-in de redirection de console. Vous pouvez télécharger un JRE à l'adresse **java.sun.com**.

△ **PRÉCAUTION : Pour réussir à lancer le média virtuel, assurez-vous d'avoir installé une version 32 bits de JRE sur un système d'exploitation 64 bits ou 32 bits. iDRAC6 ne prend *pas* en charge les navigateurs 64 bits, ni les versions JRE 64 bits. Seuls les navigateurs 32 bits dotés de versions 32 bits de JRE sont pris en charge. En outre, assurez-vous que, pour Linux, le progiciel connexe « compat-libstdc++-33-3.2.3-61 » est installé pour pouvoir lancer le média virtuel. Sous Windows, il se peut que le progiciel soit inclus dans le progiciel d'infrastructure .NET.**

---

## Configuration du média virtuel

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Sélectionnez **Système**→ onglet **Console/Média**→ **Configuration**→ **Média virtuel** pour configurer les paramètres du média virtuel.

   Le tableau 15-2 décrit les valeurs de configuration du **média virtuel**.
3. Une fois les paramètres configurés, cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 15-3.

**Tableau 15-2. Propriétés de configuration du média virtuel**

| Attribut | Valeur |
|---|---|
| Condition | **Connecter :** connecte immédiatement le **média virtuel** au serveur.<br><br>**Déconnecter :** déconnecte immédiatement le **média virtuel** du serveur.<br><br>**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** autorisées, qui est toujours fixé à 1. |
| Sessions actives | Affiche le nombre actuel de sessions de média virtuel. |
| Cryptage de média virtuel activé | Sélectionnez ou désélectionnez la case à cocher pour activer ou désactiver le cryptage des connexions du **média virtuel**. La sélection active le cryptage, la désélection désactive le cryptage. |
| Émulation de disquette | Indique si le **média virtuel** apparaît au serveur comme un lecteur de disquette ou comme une clé USB. Si **Émulation de disquette** est coché, le périphérique de **média virtuel** apparaît comme un périphérique de disquette sur le serveur. Si cette option est décochée, il apparaît comme un lecteur de clé USB.<br><br>**REMARQUE :** Dans certains environnements Windows Vista® et Red Hat®, il se peut que vous ne puissiez pas virtualiser une clé USB si **Émulation de disquette** est activé. |
| Condition de la connexion | **Connecté :** une session de média virtuel est en cours.<br><br>**Pas connecté :** aucune session de média virtuel n'est en cours. |
| Activer le démarrage unique | Cochez cette case pour activer l'option **Démarrage unique**. Utilisez cet attribut pour démarrer à partir du média virtuel. Au prochain démarrage, le système démarrera à partir du périphérique suivant dans la séquence de démarrage. Cette option déconnecte automatiquement les périphériques de **média virtuel** après le démarrage unique du système. |

**Tableau 15-3. Boutons de la page de configuration**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime les valeurs **Configuration** qui apparaissent à l'écran. |
| **Actualiser** | Recharge la page **Configuration**. |
| **Appliquer** | Enregistre les nouveaux paramètres de la page **Configuration**. |

---

## Exécution du média virtuel

△ **PRÉCAUTION : N'émettez pas une commande racreset lorsque vous exécutez une session de média virtuel. Sinon, des résultats indésirables peuvent se produire, y compris une perte de données.**

**REMARQUE :** L'application de la fenêtre Visualiseur de console doit rester active pendant que vous accédez au média virtuel.

**REMARQUE :** Effectuez les étapes suivantes pour activer Red Hat® Enterprise Linux® (version 4) pour reconnaître un périphérique SCSI avec des unités logiques (LUN) multiples :

1. Ajoutez la ligne suivante à **/ect/modprobe :**

   options scsi_mod max_luns=256

   cd /boot

   mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp

2. Redémarrez le serveur.

3. Exécutez les commandes suivantes pour afficher le CD/DVD virtuel et/ou la disquette virtuelle :

   cat /proc/scsi/scsi

**REMARQUE :** Avec le média virtuel, vous ne pouvez virtualiser qu'une seule disquette/lecteur USB/image/clé et un seul lecteur optique à partir de votre station de gestion pour une mise à disposition comme lecteur (virtuel) sur le serveur géré.

## Configurations de média virtuel prises en charge

Vous pouvez activer le média virtuel pour un seul lecteur de disquette et un seul lecteur optique. Un seul lecteur pour chaque type de média peut être virtualisé à la fois.

Les lecteurs de disquette pris en charge incluent une image de disquette ou un seul lecteur de disquette disponible. Les lecteurs optiques pris en charge incluent un seul lecteur optique disponible ou un seul fichier image ISO maximum.

### Connexion du média virtuel

Effectuez les étapes suivantes pour exécuter le média virtuel :

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion.

2. Démarrez l'interface Web iDRAC6. Pour plus d'informations, consultez « Accès à l'interface Web ».

3. Sélectionnez **Système→ Console/Média→ Redirection de console et média virtuel.**

4. La page **Redirection de console et média virtuel** s'affiche. Si vous souhaitez modifier les valeurs des attributs affichés, consultez « Configuration du média virtuel ».

   **REMARQUE : Fichier image de disquette** dans **Lecteur de disquette** (si applicable) peut apparaître, car ce périphérique peut être virtualisé comme une disquette virtuelle. Vous pouvez sélectionner simultanément un seul lecteur optique et un seul lecteur flash de disquette/USB à virtualiser.

   **REMARQUE :** Les lettres des lecteurs de périphériques virtuels sur le serveur géré ne coïncident pas avec celles des lecteurs physiques sur la station de gestion.

   **REMARQUE :** Le **média virtuel** peut ne pas fonctionner correctement sur les clients de système d'exploitation Windows qui sont configurés avec l'option de sécurité avancée d'Internet Explorer. Pour résoudre ce problème, consultez la documentation de votre système d'exploitation Microsoft ou contactez votre administrateur système.

5. 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 **KVM iDRAC6** se lance dans une fenêtre distincte.

6. Cliquez sur **Média virtuel→ Lancer le média virtuel**.

   L'assistant **Session de média virtuel** s'affiche.

   **REMARQUE :** Ne fermez pas cet assistant, sauf si vous désirez mettre fin à la session de média virtuel.

7. Si le média est connecté, vous devez le déconnecter avant de connecter une source de média différente. Décochez la case à gauche du média que vous souhaitez déconnecter.

8. Cochez la case à côté du type de média que vous souhaitez connecter.

Si vous souhaitez connecter une image de disquette ou une image ISO, saisissez le chemin (sur votre ordinateur local) de l'image ou cliquez sur le bouton **Ajouter image...** et recherchez l'image.

Le média est connecté et la fenêtre **Condition** est mise à jour.

### Déconnexion du média virtuel

1. Cliquez sur **Outils**→ **Lancer le média virtuel**.
2. Décochez la case à gauche du média que vous souhaitez déconnecter.

   Le média est déconnecté et la fenêtre **Condition** est mise à jour.
3. Cliquez sur **Quitter** pour mettre fin à l'assistant **Session de média virtuel**.

**REMARQUE :** À chaque fois qu'une session Média virtuel est lancée ou qu'un disque VFlash est connecté, un lecteur supplémentaire intitulé « LCDRIVE » s'affiche sur le système d'exploitation hôte et sur le BIOS. Le lecteur supplémentaire disparaît lorsque le disque VFlash ou la session de média virtuel est déconnecté.

## 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 répertoriés dans le bon ordre.

Pour modifier le paramètre du BIOS, effectuez les étapes suivantes :

1. Démarrez le serveur géré.
2. Appuyez sur <F2> pour accéder à 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 répertorié 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 tente de démarrer à partir d'un périphérique de démarrage en suivant l'ordre de démarrage. Si le périphérique virtuel est connecté et qu'un média de démarrage est présent, le système démarre sur le périphérique virtuel. Autrement, le système ignore le périphérique, 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 d'installation du système d'exploitation sur votre station de gestion qui peut prendre plusieurs heures. Une procédure d'installation avec script du système d'exploitation utilisant le **média virtuel** peut prendre moins de 15 minutes. Pour plus d'informations, consultez « Déploiement du système d'exploitation ».

1. Vérifiez les points suivants :
   - Le CD d'installation du système d'exploitation est inséré dans le lecteur de CD de la station de gestion.
   - Le lecteur de CD local est sélectionné.
   - Vous êtes connecté aux lecteurs virtuels.
2. Suivez les étapes de démarrage à partir du média virtuel de la section « Démarrage à partir d'un média virtuel » afin de garantir que le BIOS est défini pour démarrer à partir du lecteur de CD à partir duquel vous effectuez l'installation.
3. Suivez les instructions à l'écran pour terminer l'installation.

Pour une installation multi-disques, il est essentiel de suivre les étapes suivantes :

1. Démappez le CD/DVD virtualisé (redirigé) de la console du média virtuel.
2. Insérez le CD/DVD suivant dans le lecteur optique distant.

3. Mappez (redirigez) ce CD/DVD depuis la console du média virtuel.

   L'insertion d'un nouveau CD/DVD dans le lecteur optique distant sans remappage peut se solder par un échec.

### Fonctionnalité Démarrage unique

La fonctionnalité Démarrage unique vous aide à modifier temporairement l'ordre de démarrage afin de démarrer à partir d'un périphérique de média virtuel. Cette fonctionnalité est utilisée conjointement au média virtuel, en règle générale lors de l'installation de systèmes d'exploitation.

**REMARQUE :** Vous devez disposer de privilèges **Configuration iDRAC6** pour utiliser cette fonctionnalité.

**REMARQUE :** Les périphériques distants doivent être redirigés à l'aide du média virtuel pour utiliser cette fonctionnalité.

Pour utiliser la fonctionnalité Démarrage unique, procédez comme suit :

1. Allumez le serveur et accédez au gestionnaire de démarrage du BIOS.
2. Modifiez la séquence de démarrage afin de démarrer à partir du périphérique de média virtuel distant.
3. Ouvrez une session sur iDRAC6 par le biais de l'interface Web et cliquez sur **Système**→ **Console/Média**→ **Configuration**.
4. Cochez l'option **Activer le démarrage unique** sous Média virtuel.
5. Effectuez un cycle d'alimentation sur le serveur.

   Le serveur démarre à partir du périphérique de média virtuel distant. Au prochain redémarrage du serveur, la connexion au média virtuel distant est interrompue.

   **REMARQUE :** Le média virtuel doit être en état **connecté** pour que les lecteurs virtuels apparaissent dans la séquence de démarrage. Assurez-vous que le média de démarrage est présent dans le lecteur virtualisé pour activer le **démarrage unique**.

## Utilisation d'un média virtuel lors de 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 peuvent ne 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 concernant le média virtuel

Le tableau 15-4 répertorie les questions les plus fréquentes et les réponses.

**Tableau 15-4.** Utilisation d'un média virtuel : questions les plus fréquentes

| Question | Réponse |
|---|---|
| Je remarque parfois que ma connexion de client au média virtuel est interrompue. Pourquoi ? | Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion en déconnectant la liaison entre le serveur et le lecteur virtuel.<br><br>Si les paramètres de configuration du média virtuel sont modifiés dans l'interface Web iDRAC6 ou via les commandes de la RACADM locale, tout média connecté est déconnecté lorsque les modifications de la configuration sont appliquées.<br><br>Pour rétablir la connexion au lecteur virtuel, utilisez l'Assistant Média virtuel. |
| Quels sont les systèmes d'exploitation pris en charge par iDRAC6 ? | Consultez « Systèmes d'exploitation pris en charge » pour obtenir la liste des systèmes d'exploitation pris en charge. |
| Quels sont les navigateurs Web qui prennent en charge iDRAC6 ? | Pour accéder à la liste des navigateurs Web pris en charge, consultez « 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 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 l'IUG et continuez l'opération précédente.<br>• Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion en déconnectant la liaison 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 saisi des commandes RACADM. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité **Média virtuel**. |
| Une installation du système d'exploitation Windows via le média virtuel semble prendre trop longtemps. Pourquoi ? | Si vous installez le système d'exploitation Windows à l'aide du DVD *Dell Systems Management Tools and Documentation* et que la connexion réseau est lente, la procédure d'installation peut nécessiter beaucoup plus de temps pour accéder à l'interface Web iDRAC6 en raison de la latence du réseau. Même si la fenêtre d'installation n'indique pas la progression de l'installation, la procédure d'installation est en cours. |
| Comment puis-je configurer mon périphérique virtuel comme périphérique de démarrage ? | Sur le serveur géré, accédez à la configuration du BIOS et cliquez sur le menu de démarrage. Recherchez le CD virtuel, la disquette virtuelle ou le disque flash virtuel et changez l'ordre de démarrage des périphériques, si nécessaire. En outre, faites du périphérique virtuel un périphérique de démarrage en appuyant sur la touche « Barre d'espace » dans la séquence de démarrage de l'installation CMOS. Par exemple, pour démarrer à partir d'un lecteur de CD, définissez-le en tant que premier lecteur dans l'ordre de démarrage. |
| À partir de quels types de média puis-je démarrer ? | iDRAC6 vous permet de démarrer à partir des médias de démarrage suivants :<br>• Média de données de CD-ROM/DVD<br>• Image ISO 9660<br>• Disquette 1.44 ou image de disquette<br>• Clé USB qui est reconnue par le système d'exploitation comme disque amovible<br>• Image de clé USB |
| Comment faire pour faire de ma clé USB une clé de démarrage ? | Recherchez sur le site **support.dell.com** l'utilitaire de démarrage Dell, un programme Windows que vous pouvez utiliser pour faire de votre clé USB Dell une clé de démarrage.<br><br>Vous pouvez également démarrer à l'aide d'un disque de démarrage de Windows 98 et copier les fichiers système du disque de démarrage sur votre clé USB. Par exemple, à l'invite du DOS, tapez la commande suivante :<br><br>`sys a: x: /s`<br><br>où *x*: est la clé USB que vous voulez utiliser comme clé de démarrage. |
| Je n'arrive pas à trouver mon périphérique de disquette virtuel/CD virtuel sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou SUSE® Linux. Mon média virtuel est connecté et je suis connecté à ma disquette distante. Que dois-je faire ? | Certaines versions de Linux ne montent pas automatiquement le lecteur de disquette virtuel et le lecteur de CD virtuel de la même manière. Pour monter le lecteur de disquette virtuel, recherchez le nud de périphérique que Linux attribue au lecteur de disquette virtuel. Procédez comme suit pour rechercher et monter correctement le lecteur de disquette virtuel :<br><br>1. Ouvrez une invite de commande Linux et exécutez la commande suivante :<br><br>`grep "Virtual Floppy" /var/log/messages`<br><br>2. Recherchez la dernière entrée de ce message et notez l'heure.<br>3. À l'invite de Linux, exécutez la commande suivante :<br><br>`grep "hh:mm:ss" /var/log/messages`<br>où :<br><br>*hh:mm:ss* correspond à l'horodatage du message retourné par grep à l'étape 1.<br><br>4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique attribué à la disquette virtuelle Dell.<br>5. Assurez-vous que vous êtes relié et connecté au lecteur de disquette virtuel.<br>6. À l'invite de Linux, exécutez la commande suivante :<br><br>`mount /dev/sdx /mnt/floppy`<br><br>où :<br><br>*/dev/sdx* est le nom du périphérique trouvé à l'étape 4<br><br>/mnt/floppy est le point de montage. |
| Je n'arrive pas à trouver mon périphérique de disquette virtuel/CD virtuel sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux. Mon média virtuel est connecté et je suis connecté à ma disquette distante. Que dois-je faire ? | (suite de la réponse)<br><br>Pour monter le lecteur de CD virtuel, recherchez le nud de périphérique que Linux attribue au lecteur de CD virtuel. Suivez ces étapes pour trouver et monter le lecteur de CD virtuel :<br><br>1. Ouvrez une invite de commande Linux et exécutez la commande suivante :<br><br>`grep "Virtual CD" /var/log/messages`<br><br>2. Recherchez la dernière entrée de ce message et notez l'heure.<br>3. À l'invite de Linux, exécutez la commande suivante :<br><br>`grep "hh:mm:ss" /var/log/messages`<br><br>où<br><br>hh:mm:ss correspond à l'horodatage du message retourné par grep à l'étape 1.<br><br>4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique qui est donné à « Dell Virtual CD ».<br>5. Assurez-vous que vous êtes relié et connecté au lecteur de CD virtuel.<br>6. À l'invite de Linux, exécutez la commande suivante : |

| | |
|---|---|
| | mount */dev/sdx* /mnt/CD<br><br>où :<br><br>*/dev/sdx* est le nom du périphérique trouvé à l'étape 4<br><br>/mnt/floppy est le point de montage. |
| Lorsque j'ai effectué une mise à jour de micrologiciel à distance via l'interface Web iDRAC6, mes lecteurs virtuels présents sur le serveur ont été supprimés. Pourquoi ? | Les mises à jour de micrologiciel entraînent la réinitialisation d'iDRAC6, une interruption de la connexion à distance et le démontage des lecteurs virtuels. |
| Pourquoi tous mes périphériques USB sont-ils déconnectés après que j'ai connecté un périphérique USB ? | Les périphériques de média virtuel et les périphériques de disque flash virtuel sont connectés au BUS USB hôte comme un périphérique USB composite et ils partagent un port USB commun. À chaque fois qu'un périphérique USB de média virtuel ou de disque flash virtuel est connecté au BUS USB hôte ou déconnecté du BUS USB hôte, tous les périphériques de média virtuel et de disque flash virtuel sont momentanément déconnectés du bus hôte USB et seront par la suite reconnectés. Si un périphérique de média virtuel est utilisé par le système d'exploitation hôte, vous devez éviter de connecter ou déconnecter un ou plusieurs périphériques de média virtuel ou de disque flash virtuel. Il est recommandé de connecter d'abord tous les périphériques USB nécessaires avant de les utiliser. |
| Que fait le bouton **Réinitialisation USB ?** | Il réinitialise les périphériques USB distants et locaux connectés au serveur. |

---

Retour à la page du sommaire

Retour à la page du sommaire

# Utilisation de l'utilitaire de configuration iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



---

## Présentation

L'utilitaire de configuration iDRAC6 est un environnement de configuration de prédémarrage vous permettant d'afficher et de définir les paramètres d'iDRAC6 et du serveur géré. Vous pouvez notamment :

- afficher les numéros de révision du micrologiciel pour le micrologiciel iDRAC6 et le micrologiciel de fond de panier principal,
- activer ou désactiver le réseau local iDRAC6,
- activer ou désactiver IPMI sur LAN,
- configurer les paramètres LAN,
- activer ou désactiver la découverte automatique et configurer le serveur de provisionnement,
- configurer le média virtuel,
- configurer la carte à puce,
- changer le nom d'utilisateur et le mot de passe d'administration,
- réinitialiser les paramètres d'usine de la configuration iDRAC6,
- afficher les messages du journal des événements système (SEL) ou les effacer du journal,
- configurer l'écran LCD,
- configurer les services système.

Les tâches que vous pouvez réaliser à l'aide de l'utilitaire de configuration iDRAC6 peuvent également être exécutées avec d'autres utilitaires fournis par le logiciel iDRAC6 ou Dell™ OpenManage™, notamment l'interface Web, l'interface de ligne de commande SM-CLP ainsi que l'interface de ligne de commande RACADM locale et distante.

---

## Démarrage de l'utilitaire de configuration iDRAC6

1. Mettez sous tension ou redémarrez le serveur en appuyant sur le bouton d'alimentation situé à l'avant du serveur.
2. Lorsque le message **Appuyez sur <Ctrl-E> pour configurer l'accès à distance dans 5 s...** s'affiche, appuyez immédiatement sur <Ctrl><E>.

**REMARQUE :** Si votre système d'exploitation commence à se charger avant que vous ayez appuyé sur <Ctrl><E>, laissez le système terminer son démarrage, puis redémarrez votre serveur et réessayez.

La fenêtre **Utilitaire de configuration iDRAC6** s'affiche. Les deux premières lignes fournissent des informations sur les révisions du micrologiciel iDRAC6 et du micrologiciel du fond de panier principal. Les niveaux de révision peuvent être utiles afin de déterminer si une mise à niveau du micrologiciel est nécessaire.

Le micrologiciel iDRAC6 est la partie des informations relatives aux interfaces externes, telles que l'interface Web, SM-CLP et les interfaces 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 vers la gauche>, la <flèche vers la droite> ou sur 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 vers la gauche>, la <flèche vers la droite> et la barre d'espace pour choisir entre **Activé** et **Désactivé**.

Le LAN iDRAC6 est activé dans la configuration par défaut. Le LAN doit être activé pour permettre l'utilisation des services iDRAC6, tels que l'interface Web, Telnet/SSH, la redirection de console et le média virtuel.

Si vous choisissez de désactiver le LAN, l'avertissement suivant s'affiche :

```
iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF.

Press any key to clear the message and continue.

(L'interface hors bande iDRAC6 sera désactivée si le canal LAN est désactivé.

Appuyez sur n'importe quelle touche pour effacer le message et continuer.)
```

Le message vous informe que outre les services auxquels vous accédez en vous connectant directement aux ports 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.

## IPMI sur LAN

Appuyez sur la <flèche vers la gauche>, la <flèche vers la 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 :

```
iDRAC6 Out-of-Band IPMI interface will be disabled if IPMI Over LAN is OFF.

(L'interface IPMI hors bande iDRAC6 sera désactivée si IPMI sur LAN est désactivé.)
```

Appuyez sur n'importe quelle touche pour effacer le message et continuer. Consultez « LAN iDRAC6 » pour obtenir une explication du message.

## Paramètres LAN

Appuyez sur <Entrée> pour afficher le sous-menu Paramètres LAN. Une fois la configuration des paramètres LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

**Tableau 18-1. Paramètres LAN**

| Élément | Description |
|---|---|
| **Paramètres communs** | |
| Sélection du NIC | Appuyez sur la <flèche vers la droite>, la <flèche vers la gauche> et la barre d'espace pour basculer d'un mode à l'autre.<br><br>Les modes disponibles sont : **Dédié, Partagé**, **Partagé avec basculement LOM2** et **Partagé avec basculement tous les LOM**.<br><br>Ces modes permettent à iDRAC6 de se servir de l'interface correspondante pour communiquer avec l'extérieur. |
| Adresse Mac | Il s'agit de l'adresse MAC non modifiable de l'interface réseau iDRAC6. |
| Activation du VLAN | Sélectionnez **Activé** pour activer le filtrage du LAN virtuel pour iDRAC6. |
| Référence du VLAN | Si **Activation du VLAN** est défini sur **Activé**, saisissez une valeur Référence du VLAN entre 1 et 4 094. |
| Priorité du VLAN | Si **Activation du VLAN** est défini sur **Activé**, sélectionnez la priorité du VLAN entre 0 et 7. |
| Enregistrer le nom iDRAC6 | Sélectionnez **Activé** pour enregistrer le nom iDRAC6 auprès du service DNS. Sélectionnez **Désactivé** si vous ne voulez pas que les utilisateurs puissent trouver le nom iDRAC6 dans DNS. |
| Nom iDRAC6 | Si **Enregistrer le nom iDRAC** est défini sur **Activé**, appuyez sur <Entrée> pour modifier le champ de texte **Nom iDRAC DNS actuel**. Appuyez sur <Entrée> une fois la modification du nom iDRAC6 terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom iDRAC6 doit être un nom d'hôte DNS valide. |
| Nom de domaine de DHCP | Sélectionnez **Activé** si vous souhaitez obtenir le nom de domaine auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** si vous souhaitez spécifier le nom de domaine. |
| Nom de domaine | Si **Nom de domaine de DHCP** est défini sur **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 `masociété.com`. |
| Chaîne de nom d'hôte | Appuyez sur <Entrée> pour modifier. Saisissez le nom de l'hôte pour les alertes d'interruptions d'événements sur plateforme (PET). |
| Alerte LAN activée | Sélectionnez **Activé** pour activer l'alerte LAN PET. |
| Entrée 1 de règle d'alerte | Sélectionnez **Activer** ou **Désactiver** pour activer la première destination de l'alerte. |
| Destination de l'alerte 1 | Si **Alerte LAN activée** est défini sur **Activé**, saisissez l'adresse IP à laquelle les alertes LAN PET seront transférées. |
| **Paramètres IPv4 :** Activez ou désactivez la prise en charge de la connexion IPv4. | |

| | |
|---|---|
| IPv4 | Sélectionnez **Activé** ou **Désactivé** pour la prise en charge du protocole IPv4. |
| Clé de cryptage RMCP+ | Appuyez sur <Entrée> pour modifier la valeur et sur <Échap> lorsque vous avez terminé. La clé de cryptage RMCP+ est une chaîne hexadécimale de 40 caractères (caractères 0-9, a-f et A-F). RMCP+ est une extension IPMI qui ajoute de l'authentification et du cryptage à IPMI. La valeur par défaut est une chaîne de 40 0 (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.<br><br>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.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP que vous souhaitez attribuer à iDRAC6.<br><br>L'adresse par défaut est **192.168.0.120**. |
| Masque de sous-réseau | Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse de masque de sous-réseau obtenue auprès de DHCP.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez le masque de sous-réseau d'iDRAC6. L'adresse par défaut est **255.255.255.0**. |
| Passerelle par défaut | Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP de la passerelle par défaut. L'adresse par défaut est **192.168.0.1**. |
| Serveurs DNS de DHCP | Sélectionnez **Activé** pour récupérer les adresses de serveur DNS auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** pour spécifier les adresses de serveur DNS ci-dessous. |
| Serveur DNS 1 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du premier serveur DNS. |
| Serveur DNS 2 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du deuxième serveur DNS. |
| **Paramètres IPv6 :** Activez ou désactivez la prise en charge de la connexion IPv6. | |
| Source d'adresse IP | Choisissez entre **AutoConfig** et **Statique**. Lorsque **AutoConfig** est sélectionné, les champs **Adresse IPv6 1**, **Longueur du préfixe** et **Passerelle par défaut** sont obtenus auprès de DHCP.<br><br>Lorsque **Statique** est sélectionné, les éléments **Adresse IPv6 1**, **Longueur du préfixe** et **Passerelle par défaut** deviennent modifiables. |
| Adresse IPv6 1 | Si la **source d'adresse IP** est définie sur **AutoConfig**, ce champ affiche l'adresse IP obtenue auprès de DHCP.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP que vous souhaitez attribuer à iDRAC6. |
| Longueur du préfixe | Configure la longueur du préfixe de l'adresse IPv6. Il peut s'agir d'une valeur entre 1 et 128 inclus. |
| Passerelle par défaut | Si la **source d'adresse IP** est définie sur **AutoConfi**g, ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP de la passerelle par défaut. |
| Adresse locale de la liaison IPv6 | Il s'agit de l'**adresse locale de la liaison IPv6** non modifiable de l'interface réseau iDRAC6. |
| Adresse IPv6 2 | Il s'agit de l'**adresse IPv6 2** non modifiable de l'interface réseau iDRAC6. |
| 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 défini sur **Désactivé**, saisissez l'adresse IP du premier serveur DNS. |
| Serveur DNS 2 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du premier serveur DNS. |
| **Configurations LAN avancées** | |
| Négociation automatique | Si **Sélection NIC** est défini sur **Dédié**, choisissez entre **Activé** et **Désactivé**.<br><br>Lorsque **Activé** est sélectionné, **Paramètre de vitesse du LAN** et **Paramètre de duplex du LAN** sont automatiquement configurés. |
| Paramètre de vitesse du LAN | Si **Négociation automatique** est défini sur **Désactivé**, choisissez entre 10 Mbits/s et 100 Mbits/s. |
| Paramètre de duplex du LAN | Si **Négociation automatique** est défini sur **Désactivé**, choisissez entre **Semi-duplex** et **Duplex intégral**. |

# Configuration du média virtuel

## Média virtuel

Appuyez sur <Entrée> pour sélectionner **Déconnecté, Connecté** ou **Autoconnecté**. Lorsque vous sélectionnez **Connecté**, les périphériques de média virtuel sont connectés au bus USB, ce qui les rend disponibles lors des sessions de **redirection de console**.

Si vous sélectionnez **Déconnecté**, les utilisateurs ne peuvent pas accéder aux périphériques de média virtuel lors des sessions de **redirection de console**.

**REMARQUE :** Pour utiliser un lecteur flash USB avec la fonctionnalité **Média virtuel**, le **type d'émulation de lecteur flash USB** doit être défini sur **Disque dur** dans l'utilitaire de configuration du BIOS. L'utilitaire de configuration du BIOS est accessible en appuyant sur <F2> lors du démarrage du serveur. Si le **type d'émulation de lecteur flash USB** est défini sur **Automatique**, le lecteur flash apparaît sous forme de lecteur de disquette sur le système.

### VFlash

Appuyez sur <Entrée> pour sélectionner **Désactivé** ou **Activé**.

**Désactiver/Activer** entraîne une **déconnexion** et une **connexion** de tous les périphériques de média virtuel du bus USB.

**Désactiver** entraîne la suppression du disque flash virtuel et le rend non disponible à l'utilisation.

**REMARQUE :** Ce champ est en lecture seule si une carte SD de plus de 256 Mo n'est pas présente dans le logement de carte iDRAC6 Express.

### Formater VFlash

Choisissez cette option pour formater le disque VFlash. Le formatage effacera les données existantes sur la carte SD. Ce champ peut être modifié uniquement si une carte SD d'une taille supérieure à 256 Mo est présente dans le logement de carte iDRAC6 Enterprise.

## Ouverture de session par carte à puce

Appuyez sur <Entrée> pour sélectionner **Activé** ou **Désactivé**. Cette option permet de configurer la fonctionnalité Ouverture de session par carte à puce. Les options disponibles sont **Activé**, **Désactivé** et **Activé avec RACADM**.

**REMARQUE :** Lorsque vous sélectionnez **Activé** ou **Activé avec RACADM**, **IPMI sur LAN** est désactivé et bloqué en vue de la modification.

## Configuration des services système

### Services système

Appuyez sur <Entrée> pour sélectionner **Activé** ou **Désactivé**. Consultez le *Guide d'utilisation de Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **support.dell.com/manuals** pour plus d'informations.

**REMARQUE :** La modification de cette option entraîne le redémarrage du serveur lorsque vous utilisez **Enregistrer** et **Quitter** pour appliquer les nouveaux paramètres.

### Annuler les services système

Appuyez sur <Entrée> pour sélectionner **Non** ou **Oui**.

Lorsque vous sélectionnez **Oui**, toutes les sessions d'Unified Server Configurator sont fermées et le serveur redémarre lorsque vous utilisez **Enregistrer** et **Quitter** pour appliquer les nouveaux paramètres.

### Recueillir l'inventaire système au redémarrage

Sélectionnez **Activé** pour permettre le recueil de l'inventaire lors du démarrage. Consultez le *Guide d'utilisation de Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **support.dell.com/manuals** pour plus d'informations.

**REMARQUE :** La modification de cette option entraîne le redémarrage du serveur lorsque vous avez enregistré vos paramètres et avez quitté l'utilitaire de configuration iDRAC6.

## Configuration de l'écran LCD

Appuyez sur <Entrée> pour afficher le sous-menu **Configuration de l'écran LCD**. Une fois la configuration des paramètres de l'écran LCD terminée, appuyez sur <Échap> pour revenir au menu précédent.

**Tableau 18-2. Configuration utilisateur de l'écran LCD**

| | |
|---|---|
| Ligne 1 de l'écran LCD | Appuyez sur la <flèche vers la droite>, la <flèche vers la gauche> et la barre d'espace pour basculer d'une option à l'autre.<br><br>Cette option définit l'affichage de l'**Écran d'accueil** sur l'écran LCD selon l'une des options suivantes :<br><br>**Temp ambiante, Numéro d'inventaire, Nom d'hôte, Adresse IPv4 iDRAC6, Adresse IPv6 iDRAC6, Adresse MAC iDRAC6, Numéro de modèle, Aucun, Numéro de service, Alimentation système, Chaîne définie par l'utilisateur.** |
| Chaîne définie par l'utilisateur de l'écran LCD | Si la **Ligne 1 de l'écran LCD** est une **Chaîne définie par l'utilisateu**r, affichez ou saisissez la chaîne à afficher sur l'écran LCD.<br><br>La chaîne peut comporter 62 caractères au maximum. |
| Blocs d'alimentation du système LCD | Si la **Ligne 1 de l'écran LCD** est définie sur **Alimentation système**, sélectionnez **Watt** ou **BTU/h** pour spécifier l'unité à afficher sur l'écran LCD. |
| Unités de temp ambiante de l'écran LCD | Si la **Ligne 1 de l'écran LCD** est définie sur **Temp ambiante**, sélectionnez **Celsius** ou **Fahrenheit**pour spécifier l'unité à afficher sur l'écran LCD. |
| Affichage des erreurs de l'écran LCD | Sélectionnez **Simple** ou **SEL** (journal des événements système). |

| | |
|---|---|
| | Cette fonctionnalité permet l'affichage des messages d'erreur sur l'écran LCD dans l'un des deux formats :<br><br>Le format Simple consiste en une description, en anglais, de l'événement.<br><br>Le format SEL affiche une chaîne de texte du journal des événements système. |
| Indication du KVM distant de l'écran LCD | Sélectionnez **Activé** pour afficher le texte *KVM* à chaque fois qu'un KVM virtuel est actif sur l'unité. |
| Accès au panneau avant de l'écran LCD | Appuyez sur la <flèche vers la droite>, la <flèche vers la gauche > et la barre d'espace pour passer d'une option à l'autre : **Désactivé**, **Afficher et modifier** et **Afficher uniquement**.<br><br>Ce paramètre permet de définir le niveau d'accès utilisateur pour l'écran LCD. |

## Configuration de l'utilisateur du LAN

L'utilisateur du LAN est le compte administrateur iDRAC6, soit **root** par défaut. Appuyez sur <Entrée> pour afficher le sous-menu Configuration de l'utilisateur du LAN. Une fois la configuration de l'utilisateur du LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

**Tableau 18-3. Configuration de l'utilisateur du LAN**

| Élément | Description |
|---|---|
| Découverte automatique | La fonctionnalité Découverte automatique permet la découverte automatique de systèmes sans provisionnement sur le réseau ; elle permet en outre d'établir des références initiales *de manière sécurisée* afin que ces systèmes découverts puissent être gérés. Cette fonctionnalité permet à iDRAC6 de détecter le serveur de provisionnement. iDRAC6 et le serveur du service de provisionnement s'authentifient mutuellement. Le serveur de provisionnement distant envoie les références utilisateur afin qu'iDRAC6 crée un compte utilisateur avec ces références. Une fois le compte utilisateur créé, une console distante peut établir une communication WS-MAN avec iDRAC6 à l'aide des références spécifiées au cours du processus de découverte, puis envoyer les instructions sécurisées à iDRAC6 afin qu'il déploie un système d'exploitation à distance.<br><br>Pour plus d'informations sur le déploiement d'un système d'exploitation à distance, reportez-vous au Guide d'utilisation de *Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **support.dell.com/manuals**.<br><br>Exécutez les actions requises suivantes dans une session de l'**utilitaire de configuration iDRAC6** *séparée avant d'établir manuellement la découverte automatique :*<br><br>• Activer le NIC<br>• Activer IPv4<br>• Activer DHCP<br>• Obtenir le nom de domaine auprès de DHCP<br>• Désactiver le compte admin (compte n° 2)<br>• Obtenir l'adresse du serveur DNS auprès de DHCP<br>• Obtenir le nom de domaine DNS auprès de DHCP<br><br>Sélectionnez **Activé** pour activer la fonctionnalité Découverte automatique. Par défaut, cette option est définie sur **Désactivé**. Si vous avez commandé un système Dell doté de la fonctionnalité Découverte automatique défini sur **Activé**, iDRAC6 sur le système Dell est alors livré avec DHCP activé sans références par défaut pour l'ouverture de session à distance.<br><br>Avant l'ajout de votre système Dell au réseau et l'utilisation de la fonctionnalité Découverte automatique, assurez-vous que :<br><br>• Le serveur DHCP (protocole de configuration dynamique de l'hôte)/le système de noms de domaine (DNS) sont configurés.<br>• Les services Web de provisionnement sont installés, configurés et enregistrés. |
| Serveur de provisionnement | Ce champ est utilisé pour configurer le serveur de provisionnement. L'adresse du serveur de provisionnement peut être une combinaison d'adresses IPv4 ou de nom d'hôte, et ne doit pas dépasser 255 caractères. Chaque adresse doit être séparée par une virgule.<br><br>Si la fonctionnalité Découverte automatique est activée et une fois le processus de découverte automatique exécuté avec succès, les références utilisateur sont récupérées auprès du serveur de provisionnement configuré afin de permettre un provisionnement distant à venir.<br><br>Pour plus d'informations, consultez le *Guide d'utilisation de Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **support.dell.com/manuals**. |
| Accès au compte | Sélectionnez **Activé** pour activer le compte administrateur. Sélectionnez **Désactivé** pour désactiver le compte administrateur ou lorsque la découverte automatique est activée. |
| 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**. |
| Saisir 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 saisissez ne correspondent pas à ceux que vous avez saisis dans le champ **Saisir le mot de passe**, un message s'affiche et vous devez saisir à nouveau le mot de passe. |

## Réinitialiser les paramètres par défaut

Utilisez l'élément de menu **Réinitialiser les paramètres par défaut** pour réinitialiser tous les paramètres d'usine de tous les éléments de la configuration iDRAC6. Cette opération peut être requise, par exemple, si vous avez oublié le mot de passe utilisateur d'administration ou si vous souhaitez reconfigurer iDRAC6 à partir des paramètres par défaut.

Appuyez sur <Entrée> pour sélectionner l'élément. Le message d'avertissement suivant s'affiche :

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >

(La réinitialisation des paramètres d'usine va restaurer les paramètres utilisateur non volatiles à distance. Continuer ?

< NON (Annuler) >

< OUI (Continuer) >)
```

Sélectionnez **OUI** et appuyez sur <Entrée> pour réinitialiser les paramètres par défaut d'iDRAC6.

## Menu Journal des événements système

Le menu **Journal des événements système** vous permet d'afficher les messages du journal des événements système (SEL) et d'effacer les messages du journal. Appuyez sur <Entrée> pour afficher le menu **Journal des événements système**. Le système compte les entrées de journal, puis affiche le nombre total d'enregistrements et le message le plus récent. Le journal SEL conserve un maximum de 512 messages.

Pour afficher les messages du journal SEL, sélectionnez **Afficher le journal des événements système** et appuyez sur <Entrée>. Utilisez la <flèche vers la gauche> pour accéder au message précédent (le plus ancien) et la <flèche vers la droite> pour accéder au message suivant (le plus récent). Saisissez un numéro d'enregistrement pour atteindre cet enregistrement. Appuyez sur <Échap> lorsque vous avez fini d'afficher les messages du journal SEL.

Pour effacer le 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 **Retourner à la configuration** et appuyez sur <Entrée> pour retourner à l'utilitaire de configuration iDRAC6.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Surveillance et gestion des alertes

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Cette section explique comment surveiller iDRAC6 et fournit les procédures pour configurer votre système et iDRAC6 pour recevoir des alertes.

---

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

Pour qu'iDRAC6 puisse saisir l'écran de la dernière panne, vous devez configurer le système géré de la façon suivante.

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

2. Exécutez un système d'exploitation Microsoft® Windows® pris en charge en désélectionnant la fonctionnalité « Redémarrage automatique » de Windows dans les **paramètres de démarrage et de récupération de Windows**.

3. Activez l'écran de la dernière panne (désactivé par défaut).

   Pour activer l'écran de la dernière panne à l'aide de la RACADM locale, ouvrez une invite de commande et tapez les commandes suivantes :

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

4. Activez l'horloge de récupération automatique et choisissez **Réinitialiser**, **Mise hors tension** ou **Cycle d'alimentation** comme action de **récupération automatique**. Pour configurer l'horloge de **récupération automatique**, vous devez utiliser Server Administrator ou IT Assistant.

   Pour des informations sur la configuration de l'horloge de **récupération automatique**, consultez le *Guide d'utilisation de Server Administrator*. Pour que l'écran de la dernière panne puisse être saisi, l'horloge de **récupération automatique** doit être définie sur 60 secondes ou plus. Le paramètre par défaut est 480 secondes.

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

---

## Désactivation de l'option Redémarrage automatique de Windows

Pour que la fonctionnalité Écran de la dernière panne de l'interface Web iDRAC6 fonctionne correctement, désactivez l'option **Redémarrage automatique** sur les systèmes gérés exécutant les systèmes d'exploitation Microsoft Windows Server® 2008 et Windows Server 2003.

### Désactivation de l'option Redémarrage automatique dans Windows Server 2008

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

2. Cliquez sur **Paramètres système avancés** sous **Tâches** sur la gauche.

3. Cliquez sur l'onglet **Avancé**.

4. Sous **Démarrage et récupération**, cliquez sur **Paramètres**.

5. Désélectionnez la case à cocher **Redémarrage automatique**.

6. Cliquez sur **OK** deux fois.

### Désactivation de l'option Redémarrage automatique dans Windows Server 2003

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

2. Cliquez sur l'onglet **Avancé**.

3. Sous **Démarrage et récupération**, cliquez sur **Paramètres**.

4. Désélectionnez la case à cocher **Redémarrage automatique**.

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

---

# Configuration des événements sur plateforme

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

Les événements sur plateforme pouvant être filtrés incluent :

- Filtre d'assertion critique du ventilateur
- Filtre d'assertion d'avertissement concernant la batterie
- Filtre d'assertion critique de la batterie
- Filtre d'assertion critique de la tension discrète
- Filtre d'assertion d'avertissement concernant la température
- Filtre d'assertion critique de la température
- Filtre d'assertion critique de l'intrusion
- Filtre de dégradation de la redondance
- Filtre de perte de la redondance
- Filtre d'assertion d'avertissement concernant le processeur
- Filtre d'assertion critique du processeur
- Filtre d'absence du processeur
- Filtre d'assertion d'avertissement concernant le bloc d'alimentation
- Filtre d'assertion critique du bloc d'alimentation
- Filtre d'absence du bloc d'alimentation
- Filtre d'assertion critique du journal des événements
- Filtre d'assertion critique de la surveillance
- Filtre d'assertion d'avertissement concernant l'alimentation système
- Filtre d'assertion critique de l'alimentation système
- Filtre d'assertion d'informations concernant la carte SD discrète
- Filtre d'assertion critique de la carte SD discrète
- Filtre d'assertion d'avertissement concernant la carte SD discrète

Lorsqu'un événement sur plateforme se produit (par exemple, une panne de sonde de ventilateur), un événement système est généré et enregistré dans le journal des événements système (SEL). Si cet événement correspond à un filtre d'événement sur plateforme (PEF) dans la liste des filtres d'événements sur plateforme dans l'interface Web et que vous avez configuré ce filtre pour générer une alerte (PET ou 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 également configuré pour effectuer une action (tel qu'un redémarrage du système), l'action est effectuée.

## Configuration des filtres d'événements sur plateforme (PEF)

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

### Configuration de PEF à l'aide de l'interface Web

Pour des informations détaillées, consultez « Configuration des filtres d'événements sur plateforme (PEF) ».

### Configuration de PEF à l'aide de la CLI RACADM

1. Activez PEF.

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

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

où 1 et 1 correspondent à l'index PEF et à la sélection activer/désactiver, respectivement.

L'index PEF peut être une valeur de 1 à 22. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

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

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

2. Configurez vos actions PEF.

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

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

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

   - 0 = aucune action d'alerte
   - 1 = mise hors tension du serveur
   - 2 = redémarrage du serveur
   - 3 = cycle d'alimentation du serveur

   Par exemple, pour permettre à PEF de redémarrer le serveur, tapez la commande suivante :

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
   ```

   où 1 est l'index PEF et 2 est l'action PEF pour le redémarrage.

## Configuration de PET

### Configuration de PET à l'aide de l'interface utilisateur Web

Pour des informations détaillées, consultez « Configuration des interruptions d'événement sur plateforme (PET) ».

### Configuration de PET à l'aide de la CLI RACADM

1. Activez vos alertes globales.

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

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

2. Activez PET.

   À l'invite de commande, tapez les commandes suivantes et appuyez sur <Entrée> après chaque commande :

   ```
   IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1

   IPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 1 1
   ```

   où 1 et 1 correspondent à l'index de destination PET et à la sélection activer/désactiver, respectivement.

   L'index de destination PET peut être une valeur de 1 à 4. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

   Par exemple, pour activer PET avec l'index 4, tapez la commande suivante :

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1

   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 4 1
   ```

3. Configurez votre règle PET.

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

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <adresse_IPv4>

   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 <adresse_IPv6>
   ```

   où 1 est l'index de destination PET et <*adresse_IPv4*> et <*adresse_IPv6*> sont les adresses 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, tapez :

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

## Configuration des alertes par e-mail

### Configuration des alertes par e-mail à l'aide de l'interface utilisateur Web

Pour des informations détaillées, consultez « Configuration des alertes par e-mail ».

### Configuration des alertes par e-mail à l'aide de la CLI RACADM

1. Activez vos alertes globales.

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

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

2. Activez les alertes par e-mail.

   À l'invite de commande, tapez les commandes suivantes et appuyez sur <Entrée> après chaque commande :

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
   ```

   où 1 et 1 correspondent à l'index de destination d'e-mail et à la sélection activer/désactiver, respectivement.

   L'index de destination d'e-mail peut être une valeur de 1 à 4. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

   Par exemple, pour activer l'e-mail avec l'index 4, tapez la commande suivante :

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Configurez vos paramètres d'e-mail.

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

   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <*adresse_e-mail*>

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

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

   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 *<message_personnalisé>*

   où 1 est l'index de destination d'e-mail et *<message_personnalisé>* est le message affiché dans l'alerte par e-mail.

## Test des alertes par e-mail

La fonctionnalité Alertes par e-mail du RAC permet aux utilisateurs de recevoir des alertes par e-mail lorsqu'un événement critique se produit sur le système géré. L'exemple suivant montre comment tester la fonctionnalité Alertes par e-mail pour garantir que le RAC peut correctement envoyer des alertes par e-mail sur le réseau.

```
racadm testemail -i 2
```

**REMARQUE :** Assurez-vous que les paramètres **SMTP** et **Alerte par e-mail** sont configurés avant de tester la fonctionnalité Alertes par e-mail. Pour plus d'informations, consultez « Configuration des alertes par e-mail ».

## Test de la fonctionnalité Alerte par interruption SNMP du RAC

La fonctionnalité Alerte par interruption SNMP du RAC permet aux configurations de l'écouteur d'interruptions SNMP de recevoir des interruptions pour les événements système qui se produisent sur le système géré.

L'exemple suivant montre comment un utilisateur peut tester la fonctionnalité Alerte par interruption SNMP du RAC.

```
racadm testtrap -i 2
```

Avant de tester la fonctionnalité Alertes par interruption SNMP du RAC, assurez-vous que les paramètres SNMP et d'interruption sont configurés correctement. Consultez les descriptions des sous-commandes « **testtrap** » et « **testemail** » pour configurer ces paramètres.

# Questions les plus fréquentes concernant l'authentification SNMP

**Explication de l'affichage du message suivant :**

`Remote Access: SNMP Authentication Failure (Accès distant : échec de l'authentification SNMP)`

Pendant la découverte, IT Assistant essaie de vérifier les noms de communauté get et set du périphérique. Dans IT Assistant, le **nom de communauté get = public** et le **nom de communauté set = private**. Par défaut, le nom de communauté de l'agent iDRAC6 est **public**. Lorsqu'IT Assistant envoie une requête set, l'agent iDRAC6 génère une erreur d'authentification SNMP, car il accepte uniquement les requêtes de la **communauté = public**.

**REMARQUE :** Ce nom est celui de la communauté de l'agent SNMP utilisé pour la découverte.

Vous pouvez changer le nom de communauté iDRAC6 à l'aide de RACADM.

Pour afficher le nom de communauté iDRAC6, utilisez la commande suivante :

```
racadm getconfig -g cfgOobSnmp
```

Pour définir le nom de communauté iDRAC6, utilisez la commande suivante :

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

Pour accéder/configurer le nom de communauté de l'agent SNMP iDRAC6 à l'aide de l'interface Web, accédez à **Accès à distance**→ **Réseau/Sécurité**→ **Services** et cliquez sur **Agent SNMP**.

Pour éviter de générer des erreurs d'authentification SNMP, vous devez saisir des noms de communauté qui seront acceptés par l'agent. Comme iDRAC6 n'accepte qu'un seul nom de communauté, vous devez utiliser le même nom de communauté **get** et **set** pour configurer la découverte sous IT Assistant.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Récupération et dépannage du système géré

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Cette section explique comment utiliser l'interface Web iDRAC6 pour effectuer les tâches de récupération et de dépannage d'un système distant en panne.

- « Premières étapes de dépannage d'un système distant »
- « Gestion de l'alimentation d'un système distant »
- « Utilisation des journaux de démarrage POST »
- « Affichage de l'écran de la dernière panne système »

---

## Premières étapes de dépannage d'un système distant

Les questions suivantes aident souvent à dépanner les problèmes de haut niveau du système géré :

1. Le système est-il sous tension ou hors tension ?
2. S'il est sous tension, est-ce que le système d'exploitation fonctionne, est-il tombé en panne ou est-il seulement bloqué ?
3. S'il est hors tension, est-ce que l'alimentation a été coupée soudainement ?

Pour les systèmes en panne, consultez l'écran de la dernière panne (consultez « Affichage de l'écran de la dernière panne système ») et utilisez la redirection de console et la gestion de l'alimentation à distance (consultez « Gestion de l'alimentation d'un système distant ») pour redémarrer le système et observer le processus de redémarrage.

---

## Gestion de l'alimentation d'un système distant

iDRAC6 vous permet d'effectuer à distance plusieurs actions de gestion de l'alimentation sur le système géré de manière à récupérer le système après une panne système ou un autre événement système.

### Sélection d'actions de contrôle de l'alimentation à partir de l'interface Web iDRAC6

Pour effectuer des actions de gestion de l'alimentation à l'aide de l'interface Web, consultez « Exécution de tâches de contrôle de l'alimentation sur le serveur ».

### Sélection d'actions de contrôle de l'alimentation depuis la CLI iDRAC6

Utilisez la commande `racadm serveraction` pour effectuer des opérations de gestion de l'alimentation sur le système hôte.

```
racadm serveraction <action>
```

Les options de la chaîne <*action*> sont :

- **powerdown :** met le système géré hors tension.
- **powerup :** met le système géré sous tension.
- **powercycle :** lance une opération de cycle d'alimentation sur le système géré. Cette action est équivalente à l'enfoncement du bouton d'alimentation situé sur le panneau avant du système pour la mise hors puis sous tension du système.
- **powerstatus :** affiche l'état actuel de l'alimentation du serveur (« ACTIVÉ » ou « DÉSACTIVÉ »).
- **hardreset :** effectue une opération de réinitialisation (redémarrage) sur le système géré.

---

## Affichage des informations système

La page **Résumé du système** vous permet d'afficher des informations relatives à l'intégrité de votre système et d'autres informations iDRAC6 de base en un

coup d'il et vous fournit des liens permettant d'accéder aux pages d'informations et d'intégrité du système. En outre, vous avez la possibilité de lancer rapidement des tâches courantes à partir de cette page et d'afficher les événements récents consignés dans le journal des événements système (SEL).

Pour accéder à la page **Résumé du système**, développez l'arborescence du **système** et cliquez sur **Propriétés**→ onglet **Résumé du système**. Consultez l'*aide en ligne iDRAC6* pour plus d'informations.

La page **Détails du système** affiche des informations sur les composants système suivants :

- Châssis principal du système
- Remote Access Controller

Pour accéder à la page **Détails du système**, développez l'arborescence du **système** et cliquez sur **Propriétés**→ onglet **Détails du système**.

## Châssis principal du système

**REMARQUE :** Pour recevoir les informations sur le **nom d'hôte** et le **nom du SE**, les services iDRAC6 doivent être installés sur le système géré.

**Tableau 20-1. Informations système**

| Champ | Description |
|---|---|
| **Description** | Description du système. |
| **Version du BIOS** | Version du BIOS du système. |
| **Numéro de service** | Numéro de service du système. |
| **Nom de l'hôte** | Nom du système hôte. |
| **Nom du SE** | Système d'exploitation s'exécutant sur le système. |

**Tableau 20-2. Récupération automatique**

| Champ | Description |
|---|---|
| **Action de récupération** | Lorsqu'un blocage système est détecté, iDRAC6 peut être configuré pour effectuer l'une des actions suivantes : Pas d'action, Réinitialisation matérielle, Mise hors tension ou Cycle d'alimentation. |
| **Compte à rebours initial** | Nombre de secondes qui s'écoulent après la détection d'un blocage système avant qu'iDRAC6 n'effectue une action de récupération. |
| **Compte à rebours actuel** | Valeur actuelle, en secondes, du compte à rebours. |

**Tableau 20-3. Adresses MAC du NIC intégré**

| Champ | Description |
|---|---|
| **NIC 1** | Affiche les adresses MAC (Media Access Control) du contrôleur d'interface réseau (NIC) 1 intégré. Les adresses MAC identifient de manière unique chaque nud présent sur un réseau au niveau de la couche Media Access Control. Le NIC iSCSI (Internet Small Computer System Interface) est un contrôleur d'interface réseau dont la pile iSCSI s'exécute sur l'ordinateur hôte. Les NIC Ethernet prennent en charge la norme Ethernet câblé et se connectent au bus système du serveur. |
| **NIC 2** | Affiche les adresses MAC du NIC 2 intégré permettant de l'identifier de manière unique au sein du réseau. |
| **NIC 3** | Affiche les adresses MAC du NIC 3 intégré permettant de l'identifier de manière unique au sein du réseau. |
| **NIC 4** | Affiche les adresses MAC du NIC 4 intégré permettant de l'identifier de manière unique au sein du réseau. |

## Remote Access Controller

**Tableau 20-4. Informations sur le RAC**

| Champ | Description |
|---|---|
| **Nom** | iDRAC6 |
| **Informations produit** | Integrated Dell Remote Access Controller 6 - Entreprise |
| **Date/Heure** | Heure courante au format :<br><br>Jour Mois JJ HH:MM:SS:AAAA |
| **Version du micrologiciel** | Version du micrologiciel iDRAC6 |
| **Micrologiciel mis à jour** | Date du dernier flashage du micrologiciel au format :<br><br>Jour Mois JJ HH:MM:SS:AAAA |

| | |
|---|---|
| **Version du matériel** | Version du Remote Access Controller |
| **Adresse MAC** | Adresse Media Access Control (MAC) qui identifie de manière unique chaque nud d'un réseau. |

**Tableau 20-5. Informations sur IPv4**

| Champ | Description |
|---|---|
| **IPv4 activé** | **Oui** ou **Non** |
| **Adresse IP** | Adresse 32 bits identifiant la carte d'interface réseau (NIC) auprès d'un hôte. La valeur est affichée au format séparé par des points, par exemple 143.166.154.127. |
| **Masque de sous-réseau** | Le masque de sous-réseau identifie les parties de l'adresse IP constituant le préfixe du réseau étendu et le numéro d'hôte. La valeur est affichée au format séparé par des points, par exemple 255.255.0.0. |
| **Passerelle** | Adresse d'un routeur ou d'un commutateur. La valeur est affichée au format séparé par des points, par exemple 143.166.154.1. |
| **DHCP activé** | **Oui** ou **Non**. Indique si le protocole de configuration dynamique de l'hôte (DHCP) est activé. |
| **Utiliser DHCP pour obtenir des adresses de serveur DNS** | **Oui** ou **Non**. Indique si vous souhaitez utiliser DHCP pour obtenir des adresses de serveur DNS. |
| **Serveur DNS préféré** | Indique l'adresse IPv4 statique du serveur DNS préféré. |
| **Autre serveur DNS** | Indique l'adresse IPv4 statique de l'autre serveur DNS. |

**Tableau 20-6. Champs d'informations IPv6**

| Champ | Description |
|---|---|
| **IPv6 activé** | Indique si la pile IPv6 est activée. |
| **Adresse IP 1** | Spécifie l'adresse/la longueur de préfixe IPv6 du NIC iDRAC6. La *longueur de préfixe* est combinée avec l'adresse IP 1. Il s'agit d'un entier spécifiant la longueur de préfixe de l'adresse IPv6. Il peut s'agir d'une valeur comprise entre 1 et 128. |
| **Passerelle IP** | Spécifie la passerelle du NIC iDRAC6. |
| **Adresse locale de liaison** | Spécifie l'adresse IPv6 du NIC iDRAC6. |
| **Adresse IP 2...15** | Spécifie les adresses IPv6 supplémentaires du NIC iDRAC6, le cas échéant. |
| **Autoconfig activé** | **Oui** ou **Non.** AutoConfig permet à Server Administrator d'obtenir l'adresse IPv6 du NIC iDRAC à partir du serveur du protocole de configuration dynamique de l'hôte (DHCPv6). En outre, il désactive et vide les valeurs Adresse IP statique, Longueur de préfixe et Passerelle statique. |
| **Utiliser DHCPv6 pour obtenir des adresses de serveur DNS** | **Oui** ou **Non**. Indique si vous souhaitez utiliser DHCPv6 pour obtenir des adresses de serveur DNS. |
| **Serveur DNS préféré** | Indique l'adresse IPv6 statique du serveur DNS préféré. |
| **Autre serveur DNS** | Indique l'adresse IPv6 statique de l'autre serveur DNS. |

---

## Utilisation du journal des événements système (SEL)

La page **Journal SEL** affiche les événements critiques du système qui se produisent sur le système géré.

Pour afficher le journal des événements système :

1. Dans l'arborescence du **système**, cliquez sur **Système**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Journal des événements système**.

   La page **Journal des événements système** affiche la gravité de l'événement et fournit d'autres informations comme indiqué dans le tableau 20-7.
3. Cliquez sur le bouton approprié de la page **Journal des événements système** pour continuer (consultez le tableau 20-7).

**Tableau 20-7. Icônes indicatrices de condition**

| Icône/Catégorie | Description |
|---|---|
|  | Une coche verte indique une condition intègre (normale). |
|  | Un triangle jaune contenant 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 la condition est inconnue. |
| **Date/Heure** | Date et heure auxquelles s'est produit l'événement. Si la date n'est pas renseignée, l'événement s'est alors produit lors du démarrage du système. Le format est mm/jj/aaaa hh:mm:ss, basé sur une horloge de 24 heures. |

| | |
|---|---|
| **Description** | Brève description de l'événement |

**Tableau 20-8. Boutons de la page Journal SEL**

| Bouton | Action |
|---|---|
| **Imprimer** | Imprime le journal **SEL dans l'ordre de tri qui apparaît dans la fenêtre**. |
| **Actualiser** | Recharge la page **Journal SEL**. |
| **Effacer le journal** | Efface le **journal SEL**.<br><br>**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.<br><br>**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 du support de Microsoft à l'adresse support.microsoft.com. |

## Utilisation de la ligne de commande pour afficher le journal système

```
racadm getsel -i
```

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

```
racadm getsel <options>
```

**REMARQUE :** Si aucun argument n'est spécifié, le journal est affiché dans son intégralité.

**REMARQUE :** Consultez « getsel » pour plus d'informations sur les options que vous pouvez utiliser.

La commande **clrsel** supprime tous les enregistrements existants du journal SEL.

```
racadm clrsel
```

---

## Utilisation des journaux de démarrage POST

**REMARQUE :** Tous les journaux sont effacés une fois que vous avez redémarré iDRAC6.

La page **Saisie de démarrage** permet d'accéder aux enregistrements des trois derniers cycles de démarrage disponibles. Ils sont disposés dans l'ordre du plus récent au plus ancien. Si le serveur n'a subi aucun cycle de démarrage, le message « Aucun enregistrement disponible » ne s'affiche alors. Cliquez sur **Lire** après avoir sélectionné un cycle de démarrage disponible pour l'afficher dans une nouvelle fenêtre.

**REMARQUE :** La saisie de démarrage est prise en charge uniquement sous Java, et non sous Active-X.

Pour afficher les journaux de saisie de démarrage :

1. Dans l'arborescence du **système**, cliquez sur **Système**.
2. Cliquez sur **l'onglet** Journaux, puis sur l'onglet **Saisie de démarrage**.
3. Sélectionnez un cycle de démarrage et cliquez sur **Lire**.

   La vidéo des journaux est ouverte sur un nouvel écran.

   **REMARQUE :** Vous devez fermer une vidéo de journal de saisie de démarrage ouverte avant d'en lire une autre. Vous ne pouvez pas lire deux journaux simultanément.
4. Cliquez sur **Lecture→ Lire** pour lancer la vidéo de journal de saisie de démarrage.
5. Cliquez sur **Lecture→ Commandes de média** pour arrêter la vidéo.

**REMARQUE :** Un message vous demandant d'enregistrer un fichier **data.jnlp** au lieu d'ouvrir le visualiseur peut s'afficher. Pour résoudre ce problème, procédez comme suit dans Internet Explorer : accédez à **Outils→ Options Internet→** onglet **Avancé** et désélectionnez l'option « *Ne pas enregistrer les pages cryptées sur le disque* ».

La carte iDRAC6 Express est liée à iDRAC6 lorsque vous entrez dans l'application Unified Server Configurator (USC) en appuyant sur **F10** au cours du démarrage. Si la liaison réussit, le message suivant est consigné dans le journal SEL et dans l'écran LCD : `iDRAC6 Upgrade Successful (Mise à niveau`

d'iDRAC6 réussie). Si la liaison échoue, le message suivant est consigné dans le journal SEL et dans l'écran LCD : iDRAC6 Upgrade Failed (Échec de la mise à niveau d'iDRAC6). En outre, lorsqu'une carte iDRAC6 Express contenant un micrologiciel iDRAC6 ancien ou obsolète ne prenant pas en charge la plateforme spécifique est insérée dans la carte mère et que le système est démarré, un journal est généré sur l'écran POST : iDRAC firmware is out-of-date. Please update to the latest firmware (Le micrologiciel iDRAC est obsolète. Veuillez effectuer la mise à jour vers la version la plus récente du micrologiciel). Mettez à jour la carte iDRAC6 Express avec le dernier micrologiciel iDRAC6 pour la plateforme spécifique. Pour plus d'informations, consultez le *Guide d'utilisation de Dell Lifecycle Controller*.

---

## Affichage de l'écran de la dernière panne système

**REMARQUE :** La fonctionnalité Écran de la dernière panne exige que le système géré soit configuré avec la fonctionnalité **Récupération automatique** dans Server Administrator. De plus, assurez-vous que la fonctionnalité **Récupération automatique du système** est activée à l'aide d'iDRAC6. Naviguez vers la page **Services** dans l'onglet **Réseau/Sécurité** de la section **Accès à distance** pour activer cette fonctionnalité.

La page **Écran de la dernière panne** affiche l'écran de la dernière panne le plus récent. Les informations sur la dernière panne système sont enregistrées dans la mémoire d'iDRAC6 et sont accessibles à distance.

Pour afficher la page **Écran de la dernière panne** :

1. Dans l'arborescence du **système**, cliquez sur **Système**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Écran de la dernière panne**.

La page **Écran de la dernière panne** est dotée des boutons suivants (consultez le tableau 20-9) en haut à droite de l'écran :

**Tableau 20-9. Boutons de la page Écran de la dernière panne**

| Bouton | Action |
|---|---|
| **Imprimer** | Imprime la page **Écran de la dernière panne**. |
| **Actualiser** | Recharge la page **Écran de la dernière panne**. |

**REMARQUE :** En raison des fluctuations dans l'horloge de récupération automatique, l'**écran de la dernière panne** peut ne pas être saisi lorsque l'horloge de réinitialisation du système est définie sur une valeur inférieure à 30 secondes. Utilisez Server Administrator ou IT Assistant pour définir l'horloge de réinitialisation du système sur 30 secondes au moins et vous assurer que l'**écran de la dernière panne** fonctionne correctement. Pour plus d'informations, consultez « Configuration du système géré pour la saisie de l'écran de la dernière panne ».

---

Retour à la page du sommaire

Retour à la page du sommaire

# Récupération et dépannage d'iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Cette section explique comment effectuer des tâches liées à la récupération et au dépannage d'un iDRAC6 en panne.

Vous pouvez utiliser un des outils suivants pour dépanner votre iDRAC6 :

- Journal du RAC
- Console de diagnostics
- Serveur d'identification
- Journal de suivi
- racdump
- coredump

---

## Utilisation du journal du RAC

Le **journal du RAC** est un journal permanent conservé dans le micrologiciel iDRAC6. Le journal contient une liste des actions d'utilisateur (ouverture et fermeture de session,et modifications des règles de sécurité, par exemple) et des alertes émises par iDRAC6. Les entrées les plus anciennes sont écrasées quand le journal est plein.

Pour accéder au journal du RAC depuis l'interface utilisateur (IU) iDRAC6 :

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Journal iDRAC**.

Le **journal iDRAC** contient les informations répertoriées dans le tableau 21-1.

**Tableau 21-1. Informations sur la page Journal iDRAC**

| Champ | Description |
|---|---|
| **Date/Heure** | Date et heure (par exemple, Dec 19 16:55:47).<br><br>Lorsque iDRAC6 démarre à l'initiale et qu'il ne parvient pas à communiquer avec le système géré, l'heure est affichée comme Démarrage du système. |
| **Source** | Interface qui a provoqué l'événement. |
| **Description** | Description brève de l'événement et nom d'utilisateur qui a ouvert une session sur iDRAC6. |

### Utilisation des boutons de la page Journal iDRAC

La page **Journal iDRAC** contient les boutons répertoriés dans le tableau 21-2.

**Tableau 21-2. Boutons du journal iDRAC**

| Bouton | Action |
|---|---|
| **Imprimer** | Imprime la page **Journal iDRAC**. |
| **Effacer le journal** | Efface les entrées du **journal iDRAC**.<br><br>**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 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 du support de Microsoft à l'adresse **support.microsoft.com**. |
| **Actualiser** | Recharge la page **Journal iDRAC**. |

## Utilisation de la ligne de commande

Utilisez la commande `getraclog` pour afficher les entrées du journal iDRAC6.

```
racadm getraclog -i
```

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

```
racadm getraclog [options]
```

**REMARQUE :** Pour plus d'informations, consultez « getraclog ».

Vous pouvez utiliser la commande `clrraclog` pour effacer toutes les entrées du journal iDRAC.

```
racadm clrraclog
```

## Utilisation de la console de diagnostics

iDRAC6 fournit un ensemble standard d'outils de diagnostic réseau (consultez le tableau 21-3) qui sont semblables aux outils fournis avec les systèmes Microsoft® Windows® ou Linux. À l'aide de l'interface Web iDRAC6, vous pouvez accéder aux outils de débogage réseau.

Pour accéder à la page **Console de diagnostics :** Dans l'arborescence du **système**, cliquez sur **Accès à distance**→ onglet **Dépannage**→ **Console de diagnostics**.

Le tableau 21-3 décrit les options disponibles sur la page **Console de diagnostics**. Tapez une commande et cliquez sur **Envoyer**. Les résultats du débogage apparaissent sur la page **Console de diagnostics**.

Pour actualiser la page **Console de diagnostics**, cliquez sur **Actualiser**. Pour exécuter une autre commande, cliquez sur **Retour à la page Diagnostics**.

**Tableau 21-3. Commandes de diagnostic**

| Commande | Description |
|---|---|
| **arp** | Affiche le contenu de la table du protocole de résolution d'adresses (ARP). Les entrées ARP ne peuvent être ni ajoutées, ni supprimées. |
| **ifconfig** | Affiche le contenu de la table d'interface réseau. |
| **netstat** | Imprime le contenu de la table de routage. Si le numéro optionnel de l'interface est indiqué dans le champ de texte à droite de l'option **netstat**, netstat imprime des informations supplémentaires concernant le trafic sur l'interface, l'utilisation du tampon et d'autres informations sur l'interface réseau. |
| **ping** ***<adresse IP>*** | Vérifie que l'adresse IP de destination est accessible à partir d'iDRAC6 avec le contenu actuel de la table de routage. Une adresse IP de destination doit être saisie 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 iDRAC6. Pour plus d'informations, consultez « gettracelog ». |

## Utilisation du serveur d'identification

La page **Identifier** vous permet d'activer la fonctionnalité Identification du système.

Pour identifier le serveur :

1. Cliquez sur **Système**→ **Accès à distance**→ **Dépannage**→ **Identifier.**
2. Sur l'écran **Identifier**, sélectionnez la case à cocher **Identifier le serveur** pour activer le clignotement de l'écran LCD et la LED de serveur d'identification arrière.
3. Le champ **Délai d'attente d'identification du serveur** affiche le nombre de secondes durant lesquelles l'écran LCD clignote. Saisissez la durée (en secondes) durant laquelle vous souhaitez que l'écran LCD clignote. La plage du délai d'attente est comprise entre 1 et 255 secondes. Si le délai d'attente est défini sur 0 seconde, l'écran LCD clignote de manière continue.
4. Cliquez sur **Appliquer**.

Si vous avez saisi **0** seconde, effectuez les étapes suivantes pour le désactiver :

1. Cliquez sur **Système**→ **Accès à distance**→ **Dépannage**→ **Identifier.**

2. Sur l'écran **Identifier**, désélectionnez l'option **Identifier le serveur**.

Cliquez sur **Appliquer.**

---

## Utilisation du journal de suivi

Le journal de suivi interne iDRAC6 est utilisé par les administrateurs pour déboguer les problèmes d'alerte et de mise en réseau d'iDRAC6.

Pour accéder au journal de suivi depuis l'interface Web iDRAC6 :

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Diagnostics**.
3. Tapez la commande **gettracelog** ou la commande **racadm gettracelog** dans le champ **Commande.**

   **REMARQUE :** Vous pouvez également utiliser cette commande à partir de l'interface de ligne de commande. Pour plus d'informations, consultez « gettracelog ».

Le journal de suivi enregistre les informations suivantes :

- DHCP : effectue le suivi des paquets envoyés à un serveur DHCP et reçus de celui-ci.
- IP : effectue le suivi des paquets IP envoyés et reçus.

Le journal de suivi peut en outre contenir des codes d'erreur spécifiques au micrologiciel iDRAC6 qui sont liées au micrologiciel iDRAC6 interne, et non pas au système d'exploitation du système géré.

**REMARQUE :** iDRAC6 ne renvoie pas d'ICMP (ping) si la taille du paquet dépasse 1 500 octets.

---

## Utilisation de racdump

La commande `racadm racdump` fournit une commande unique pour obtenir des informations sur le vidage et la condition ainsi que des informations générales sur la carte iDRAC6.

**REMARQUE :** Cette commande est disponible uniquement sur les interfaces Telnet et SSH. Pour plus d'informations, consultez la commande « racdump ».

---

## Utilisation de coredump

La commande `racadm coredump` affiche des informations détaillées concernant les problèmes critiques récents qui se sont produits avec le RAC. Les informations coredump peuvent être utilisées pour diagnostiquer ces problèmes critiques.

Si disponibles, les informations coredump sont permanentes sur les cycles d'alimentation du RAC et restent disponibles jusqu'à ce qu'une des conditions suivantes se produise :

- Les informations coredump sont effacées avec la sous-commande `coredumpdelete`.
- Une autre condition critique se produit sur le RAC. Dans ce cas, les informations coredump portent sur la dernière erreur critique qui s'est produite.

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

Consultez les sous-commandes « coredump » et « coredumpdelete » pour plus d'informations.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Capteurs

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Les capteurs ou sondes de matériel vous aident à surveiller les systèmes sur votre réseau plus efficacement en vous permettant de prendre les mesures appropriées pour prévenir les sinistres, tels que l'instabilité ou les dommages du système.

Vous pouvez utiliser iDRAC6 pour surveiller les capteurs de matériel pour les batteries, les sondes de ventilateurs, l'intrusion dans le châssis, les blocs d'alimentation, l'alimentation consommée, la température et les tensions.

---

## Sondes de batterie

Les sondes de batterie donnent des informations concernant les batteries de CMOS de la carte système et de la mémoire vive sur la carte mère (ROMB) de stockage.

**REMARQUE :** Les paramètres de la batterie ROMB de stockage sont disponibles uniquement si le système dispose d'une ROMB.

---

## Sondes de ventilateurs

Le capteur de la sonde du ventilateur donne des informations concernant :

- La redondance du ventilateur : la capacité du ventilateur secondaire à remplacer le ventilateur primaire si celui-ci n'arrive pas à dissiper la chaleur à une vitesse prédéfinie.
- La liste des sondes de ventilateurs : fournit des informations concernant la vitesse de ventilation de tous les ventilateurs du système.

---

## Sondes d'intrusion dans le châssis

Les sondes d'intrusion dans le châssis indiquent la condition du châssis, que celui-ci soit ouvert ou fermé.

---

## Sondes des blocs d'alimentation

Les sondes des blocs d'alimentation fournissent des informations concernant :

- La condition des blocs d'alimentation
- La redondance du bloc d'alimentation, c'est-à-dire la capacité du bloc d'alimentation redondant à remplacer le bloc d'alimentation primaire si celui-ci fonctionne mal.

**REMARQUE :** S'il n'y a qu'un seul bloc d'alimentation dans le système, la redondance du bloc d'alimentation sera définie sur **Désactivé**.

---

## Sondes de surveillance de l'alimentation

La surveillance de l'alimentation donne des informations concernant la consommation d'alimentation en *temps réel*, en watts et en ampères.

Vous pouvez également afficher une représentation graphique de la consommation d'alimentation de la dernière minute, de la dernière heure, du dernier jour ou de la dernière semaine à partir de l'heure actuelle définie dans iDRAC6.

---

## Sonde de température

Le capteur de température donne des informations concernant la température ambiante de la carte système. La sonde de température indique si la condition de la sonde entre dans la valeur prédéfinie de seuil critique et d'avertissement.

---

## Sondes de tension

Les sondes de tension types sont les suivantes. Votre système est peut-être dotés de celles-ci et/ou d'autres.

- CPU [n] VCORE
- System Board 0.9V PG
- System Board 1.5V ESB2 PG
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

Les sondes de tension indiquent si la condition des sondes entre dans la valeur prédéfinie de seuil critique et d'avertissement.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Mise en route avec iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**

iDRAC6 vous permet de surveiller, dépanner et réparer à distance un système Dell, même lorsque celui-ci est en panne. iDRAC6 est doté d'un vaste jeu de fonctionnalités incluant la redirection de console, le média virtuel, le KVM virtuel, l'authentification par carte à puce et la connexion directe.

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

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

Pour configurer iDRAC6, effectuez les étapes générales suivantes :

**REMARQUE :** Cette procédure peut différer selon les systèmes. Consultez le *Manuel du propriétaire du matériel* de votre système sur le site Web du support de Dell à l'adresse **support.dell.com / manuals** pour obtenir des instructions précises sur la réalisation de cette procédure.

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

---

Retour à la page du sommaire

Retour à la page du sommaire

# Activation de l'authentification Kerberos

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Kerberos est un protocole d'authentification de réseau qui permet aux systèmes de communiquer en toute sécurité sur un réseau non sécurisé. Pour cela, il permet aux systèmes de prouver leur authenticité. Pour se conformer aux normes de mise en application d'authentification plus rigoureuses, iDRAC6 prend désormais en charge l'authentification Active Directory® Kerberos afin de pouvoir prendre en charge les ouvertures de session par carte à puce Active Directory et par connexion directe Active Directory.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® et Windows Server 2008 utilisent Kerberos comme méthode d'authentification par défaut.

iDRAC6 utilise Kerberos pour prendre en charge deux types de mécanisme d'authentification : les ouvertures de session par connexion directe Active Directory et les ouvertures de session par carte à puce Active Directory. Pour l'ouverture de session par connexion directe, iDRAC6 utilise les références d'utilisateur mises en cache dans le système d'exploitation après que l'utilisateur a ouvert une session avec un compte Active Directory valide.

Pour l'ouverture de session par carte à puce Active Directory, iDRAC6 utilise l'authentification bifactorielle (TFA) s'articulant autour de la carte à puce comme références pour activer une ouverture de session Active Directory. Voici la fonctionnalité de suivi de l'authentification par carte à puce locale.

L'authentification Kerberos sur iDRAC6 échoue si l'heure d'iDRAC6 diffère de celle du contrôleur de domaine. Un décalage maximum de 5 minutes est autorisé. Pour que l'authentification réussisse, synchronisez l'heure du serveur avec celle du contrôleur de domaine, puis **réinitialisez** iDRAC6.

Vous pouvez également utiliser la commande de décalage du fuseau horaire RACADM suivante pour synchroniser l'heure :

```
racadm config -g cfgRacTuning -o

cfgRacTuneTimeZoneOffset <valeur de décalage>
```

---

## Spécifications de l'authentifications d'ouverture de session par connexion directe et Active Directory avec carte à puce

- Configurez iDRAC6 en vue de l'ouverture de session Active Directory. Pour plus d'informations, consultez « Utilisation de Microsoft Active Directory pour ouvrir une session sur iDRAC6 ».
- Enregistrez iDRAC6 comme un ordinateur dans le domaine racine Active Directory.
  a. Cliquez sur **Accès à distance**→ onglet **Réseau/Sécurité**→ **sous-onglet Réseau**.
  b. Fournissez une adresse IP valide pour le **serveur DNS préféré/l'autre serveur DNS**. Cette valeur est l'adresse IP du DNS faisant partie du domaine racine et authentifiant les comptes Active Directory des utilisateurs.
  c. Sélectionnez **Enregistrer iDRAC auprès du DNS.**
  d. Spécifiez un **nom de domaine DNS** valide.

  Consultez l'*aide en ligne d'iDRAC6* pour plus d'informations.

Pour prendre en charge les deux nouveaux types de mécanisme d'authentification, iDRAC6 prend en charge la configuration pour se définir en tant que service « kerberisé » sur un réseau Windows Kerberos. La configuration Kerberos sur iDRAC6 requiert les mêmes étapes que celles effectuées pour la configuration d'un service autre que Windows Server Kerberos en tant que principe de sécurité au sein de Windows Server Active Directory.

L'outil **ktpass** Microsoft (fourni par Microsoft sur le CD/DVD d'installation du serveur) sert à créer les liaisons du nom du service principal (SPN) sur un compte d'utilisateur et à exporter les informations d'approbation dans un fichier *keytab* Kerberos de style MIT, permettant ainsi d'établir une relation de confiance entre un utilisateur ou système externe et le KDC (Key Distribution Centre). Le fichier keytab contient une clé cryptographique qui sert à crypter les informations entre le serveur et le KDC. L'outil ktpass permet aux services s'articulant autour d'UNIX qui prennent en charge l'authentification Kerberos d'utiliser les fonctionnalités d'interopérabilité fournies par un service KDC Windows Server Kerberos.

Le fichier keytab généré par l'utilitaire ktpass est mis à la disposition d'iDRAC6 en tant que téléversement de fichier et est activé pour devenir un service « kerberisé » sur le réseau.

Étant donné qu'iDRAC6 est un périphérique avec un système d'exploitation autre que Windows, exécutez l'utilitaire **ktpass** (qui fait partie de Microsoft Windows) sur le contrôleur de domaine (serveur Active Directory) où vous souhaitez mapper iDRAC6 à un compte d'utilisateur dans Active Directory.

Par exemple, utilisez la commande **ktpass** suivante pour créer le fichier keytab Kerberos :

```
C:\>ktpass -princ HOST/dracname.domainname.com@DOMAINNAME.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

Le type de cryptage qu'iDRAC6 utilise pour l'authentification Kerberos est DES-CBC-MD5. Le type principal est KRB5_NT_PRINCIPAL. Les propriétés suivantes du compte utilisateur auquel le nom principal du service est mappé doivent être activées :

- Utiliser les types de cryptage DES pour ce compte
- Ne pas demander la pré-authentification Kerberos

**REMARQUE :** Il est recommandé d'utiliser le dernier utilitaire **ktpass** pour créer le fichier keytab.

Cette procédure génère un fichier keytab que vous devez téléverser vers iDRAC6.

**REMARQUE :** Le fichier keytab contient une clé de cryptage et doit être conservé en lieu sûr.

Pour plus d'informations sur l'utilitaire **ktpass**, consultez le site Web de Microsoft à l'adresse :
**http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

- L'heure d'iDRAC6 doit être synchronisée avec celle du contrôleur de domaine Active Directory.

---

## Configuration d'iDRAC6 pour l'authentification de l'ouverture de session par connexion directe et Active Directory avec carte à puce

Téléversez le fichier keytab obtenu à partir du domaine racine Active Directory vers iDRAC6 :

1. Cliquez sur **Accès à distance**→ onglet **Réseau/Sécurité**→ sous-onglet **Service de répertoire**→cliquez sur **Microsoft Active Directory**.
2. Sélectionnez **Téléverser le fichier keytab Kerberos**, puis cliquez sur **Suivant**.
3. Dans la page **Téléversement du fichier keytab Kerberos**, sélectionnez le fichier keytab à téléverser, puis cliquez sur **Appliquer**.

Vous pouvez également téléverser le fichier vers iDRAC6 à l'aide des commandes racadm de la CLI. La commande suivante permet de téléverser le fichier keytab vers iDRAC6 :

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

où <nom de fichier> est le nom du fichier keytab. La commande racadm est prise en charge par la racadm locale et distante.

---

## Configuration des utilisateurs Active Directory pour l'ouverture de session par connexion directe

Avant d'utiliser la fonctionnalité d'ouverture de session par connexion directe Active Directory, assurez-vous que vous avez déjà configuré iDRAC6 pour l'ouverture de session Active Directory et que le compte d'utilisateur de domaine à utiliser pour ouvrir une session sur le système a été activé pour l'ouverture de session Active Directory sur iDRAC6.

En outre, assurez-vous que vous avez activé le paramètre d'ouverture de session Active Directory. Consultez « Utilisation du service de répertoire iDRAC6 » pour plus d'informations sur la configuration des utilisateurs Active Directory. Vous devez également activer iDRAC6 pour qu'il devienne un service « kerberisé » en téléversant un fichier *keytab* valide, obtenu auprès du domaine racine Active Directory, vers iDRAC6.

Consultez « Configuration d'iDRAC6 pour utiliser la connexion directe » pour plus d'informations sur la façon d'activer la connexion directe à l'aide de l'IUG et de la CLI.

---

## Ouverture de session sur iDRAC6 avec la connexion directe pour les utilisateurs Active Directory

**REMARQUE :** Pour ouvrir une session sur iDRAC6, vérifiez que vous disposez des derniers composants au moment de l'exécution des bibliothèques Microsoft Visual C++ 2005. Pour plus d'informations, consultez le site Web de Microsoft.

1. Ouvrez une session sur votre système avec un compte Active Directory valide.
2. Tapez l'adresse Web d'iDRAC6 dans la barre d'adresse de votre navigateur.

   **REMARQUE :** Selon les paramètres de votre navigateur, il se peut que vous soyez invité à télécharger et installer le plug-in ActiveX de connexion directe lorsque vous utilisez cette fonctionnalité pour la première fois.

   Vous avez ouvert une session sur iDRAC6 avec les privilèges Microsoft Active Directory appropriés si :

   - vous êtes un utilisateur Microsoft Active Directory,
   - vous êtes configuré dans iDRAC6 comme pouvant ouvrir une session Active Directory,
   - iDRAC6 est activé pour l'authentification Active Directory Kerberos.

---

## Configuration des utilisateurs Active Directory pour l'ouverture de session par carte à puce

Avant d'utiliser la fonctionnalité d'ouverture de session par carte à puce Active Directory, assurez-vous d'avoir déjà configuré iDRAC6 pour l'ouverture de session Active Directory et vérifiez que le compte d'utilisateur pour lequel la carte à puce a été émise a été activé en vue de l'ouverture de session Active Directory iDRAC6.

En outre, assurez-vous que vous avez activé le paramètre d'ouverture de session Active Directory. Consultez « Utilisation du service de répertoire iDRAC6 » pour plus d'informations sur la configuration des utilisateurs Active Directory. Vous devez également activer iDRAC6 pour lui permettre de devenir un service « kerberisé » en téléversant un fichier *keytab* valide, obtenu auprès du domaine racine Active Directory, vers iDRAC6.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration de la carte de média VFlash pour une utilisation avec iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



La carte de média VFlash est une carte SD (Secure Digital) qui se branche dans le logement de carte iDRAC6 Enterprise en option à l'arrière de votre système. Elle offre un espace de stockage et se comporte comme une clé de mémoire flash USB courante. Pour plus d'informations sur l'installation et le retrait de la carte de média VFlash de votre système, consultez le *Manuel du propriétaire du matériel* à l'adresse **support.dell.com/manuals**.

---

## Configuration de la carte de média VFlash à l'aide de l'interface Web iDRAC6

### Propriétés de la carte SD

**REMARQUE :** Cette section s'affiche uniquement si une carte SD dotée de capacités de lecture/écriture est insérée dans le logement de carte SD du serveur. Dans le cas contraire, le message suivant s'affiche :

```
SD card not detected. Please insert an SD card of size 256MB or greater.

(Carte SD non détectée. Insérez une carte SD d'une taille supérieure ou égale à 256 Mo.)
```

1. Assurez-vous que la carte de média VFlash a été installée.
2. Ouvrez une fenêtre de navigateur Web pris en charge et ouvrez une session sur l'interface Web iDRAC6.
3. Dans l'arborescence du système, sélectionnez **Système**.
4. Cliquez sur l'onglet **VFlash**.

L'écran **VFlash** s'affiche.

Le tableau 16-1 répertorie les options **Propriétés de la carte SD**.

**Tableau 16-1. Propriétés de la carte SD**

| Attribut | Description |
|---|---|
| Taille de clé virtuelle | Ce champ vous permet de sélectionner la taille qui sera occupée par la clé VFlash sur la carte SD. Sélectionnez une taille de clé virtuelle et cliquez sur **Appliquer**. La clé virtuelle se réinitialise à la taille spécifiée, efface toutes les données existantes et formate une partie de la carte SD.<br><br>**REMARQUE :** Si vous avez inséré une carte SD sous licence de 1 Go, vous pouvez sélectionner 256 Mo ou 512 Mo comme taille de partition. Si vous avez inséré une carte SD sans licence d'une taille quelconque, vous pouvez sélectionner uniquement 256 Mo comme taille de partition.<br><br>Si vous avez téléversé une image avec WS-MAN, la taille de partition maximale que vous obtenez dépend de la taille de l'image. Par exemple, si vous avez téléversé une image de 500 Mo, une taille de clé virtuelle de 1 Go ne peut pas être créée avec une carte sous licence de 1 Go, car 500 Mo sont déjà utilisés par l'image. Dans ce cas, cliquez sur le bouton **Initialiser** pour réinitialiser la carte, puis sélectionnez 1 Go comme taille de clé virtuelle. |
| Type de média | Indique si une carte SD de marque Dell ou autre que Dell est insérée dans le logement de carte SD du serveur.<br><br>Si la carte SD est sous licence, la mention VFlash Dell suivie de la taille de la carte SD s'affiche. Si la carte est sans licence, la mention Carte SD autre que Dell s'affiche. |
| Image | Affiche le nom du fichier image créé sur la carte SD. Il est utilisé en tant que disque VFlash. |
| Fichier de référence | Affiche le nom du fichier texte créé sur la carte SD. Il fournit des informations relatives à l'image VFlash. |
| Connexion VFlash | Cochez cette option pour connecter le disque VFlash. Cette action permet d'exposer le fichier image **ManagedStore.IMG** créé sur la carte SD en tant que clé USB de la taille sélectionnée.<br><br>**REMARQUE :** Vous pouvez connecter le disque VFlash uniquement si une image **ManagedStore.IMG** valide est présente sur la carte SD. |
| Initialiser | Cliquez sur **Initialiser** pour créer l'image VFlash, **ManagedStore.IMG**, sur la carte SD.<br><br>**REMARQUE :** L'option **Initialiser** est activée uniquement si une carte de média VFlash est présente. En outre, la carte SD peut être formatée |

| | |
|---|---|
| | uniquement si l'option **Connexion VFlash** est décochée.<br><br>**REMARQUE :** Les fichiers **ManagedStore.IMG** et **ManagedStore.ID** qui s'affichent sur la page IUG VFlash ne sont pas visibles sur le système d'exploitation du serveur hôte, mais sur la carte SD.<br><br>**PRÉCAUTION : Lorsque vous téléversez un fichier image volumineux, si vous cliquez à un endroit quelconque, actualisez la page ou retournez sur la page VFlash, le message** « `SD card unavailable, used by another application` » (`Carte SD non disponible, utilisée par une autre application`) **risque de s'afficher. Selon la partition ou la taille du fichier image sélectionnée, ce message peut rester affiché pendant deux heures maximum.** |
| Appliquer | Enregistre la configuration actuelle. Si vous modifiez la taille de la clé virtuelle avec le menu déroulant, cliquez sur **Appliquer** pour créer une nouvelle clé virtuelle de la taille spécifiée. Toutes les données existantes seront effacées. Cette opération peut prendre quelques minutes en fonction de la taille de la clé virtuelle sélectionnée. |

## Disque VFlash

**REMARQUE :** La fonctionnalité Téléversement du fichier image est disponible uniquement si une image **ManagedStore.IMG** valide est présente sur la carte SD et si l'option **Connexion VFlash** est décochée.

Le tableau 16-2 répertorie les paramètres **Disque VFlash**.

**Tableau 16-2. Disque VFlash**

| Attribut | Description |
|---|---|
| Fichier image | Sélectionnez un fichier local sur l'ordinateur client à exposer en tant que clé USB VFlash sur le serveur distant. Vous pouvez stocker les images de démarrage d'urgence et les outils de diagnostic directement sur le média VFlash. Le fichier image peut être une image de disquette de démarrage DOS, par exemple un fichier ***.img** pour Windows® ou un fichier **diskboot.img** émanant du média Red Hat® Enterprise Linux® pour Linux. Vous pouvez utiliser **diskboot.img** pour créer un disque de secours ou un disque permettant d'effectuer des installations réseau. Vous pouvez utiliser VFlash pour héberger une image persistante à des fins d'utilisation générale ou d'urgence dans le futur. |
| Téléverser | Cliquez sur cette option pour téléverser le fichier image sélectionné sur la carte SD. Une fois le téléversement terminé, le fichier image est stocké sur la carte SD en tant que **ManagedStore.IMG**.<br><br>**REMARQUE :** Le téléversement d'images ISO n'est pas pris en charge dans cette version et peut générer des erreurs. |

**PRÉCAUTION : Vous ne serez pas en mesure d'éjecter le disque flash virtuel du système d'exploitation Windows au sein du serveur géré en cliquant avec le bouton droit de la souris sur le disque et en sélectionnant l'option « Éjecter ». Pour retirer le disque en toute sécurité, utilisez l'option fournie dans la barre d'état système dans le coin inférieur droit de votre système.**

Si vous cliquez sur un bouton de la page VFlash lorsqu'une application comme le fournisseur WSMAN, l'utilitaire de configuration iDRAC6 ou RACADM utilise VFlash, ou si vous naviguez vers une autre page de l'IUG, iDRAC6 risque d'afficher une page vierge avec le message « `VFlash is currently in use by another process. Try again after some time` » (`VFlash est actuellement utilisé par un autre processus. Réessayez ultérieurement`).

## Affichage de la taille de clé flash virtuelle

Le menu déroulant **Taille de clé virtuelle** affiche le paramètre de taille actuel.

---

# Configuration de la carte de média VFlash à l'aide de RACADM

## Activation ou désactivation de la carte de média VFlash

Ouvrez une console locale sur le serveur, puis une session et saisissez :

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 ou 0 ]
```

où `1` signifie activé et `0` signifie désactivé.

**REMARQUE :** Pour plus d'informations sur cfgRacVirtual, y compris le détail des résultats renvoyés, consultez « cfgRacVirtual ».

**REMARQUE :** La commande RACADM fonctionne uniquement si une carte de média VFlash est présente. Si aucune carte n'est présente, le message suivant s'affiche : *ERREUR : Impossible d'effectuer l'opération demandée. Assurez-vous qu'une carte SD non protégée en écriture est insérée*.

## Réinitialisation de la carte de média VFlash

Ouvrez une console texte Telnet/SSH sur le serveur, ouvrez une session et saisissez :

```
racadm vmkey reset
```

**PRÉCAUTION : La réinitialisation de la carte de média VFlash à l'aide de la commande RACADM permet de réinitialiser la taille de la clé sur 256 Mo et de supprimer toutes les données existantes.**

**REMARQUE :** Pour plus d'informations sur vmkey, consultez « vmkey ». La commande RACADM fonctionne uniquement si une carte de média VFlash est présente. Si aucune carte n'est présente, le message suivant s'affiche : *ERREUR : Impossible d'effectuer l'opération demandée. Assurez-vous qu'une carte SD est insérée*.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Surveillance et gestion de l'alimentation

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Les systèmes Dell™ PowerEdge™ intègrent de nombreuses nouvelles fonctionnalités améliorées de gestion de l'alimentation. La plateforme entière, du matériel au micrologiciel en passant par le logiciel de gestion de systèmes, a été conçue dans l'optique de réduire, de surveiller et de gérer l'alimentation.

La conception du matériel de base a été optimisée selon la perspective de l'alimentation :

- Des blocs d'alimentation haute performance et des régulateurs de tension ont été incorporés dans la conception.
- Le cas échéant, des composants dotés d'une consommation inférieure ont été sélectionnés.
- La conception du châssis optimise l'écoulement de l'air à travers le système pour réduire la puissance de ventilation.

Les systèmes PowerEdge comportent de nombreuses fonctionnalités de contrôle et de gestion de l'alimentation.

- **Inventaire de l'alimentation et bilan de puissance :** au démarrage, un inventaire système permet de calculer un bilan de puissance système de la configuration actuelle.
- **Plafonnement de l'alimentation :** les systèmes peuvent comporter un limiteur pour maintenir un plafond d'alimentation spécifié.
- **Surveillance de l'alimentation :** iDRAC6 interroge les blocs d'alimentation pour recueillir des mesures d'alimentation. iDRAC6 recueille un historique des mesures d'alimentation et calcule les moyennes d'exploitation et les crêtes. À l'aide de l'interface Web iDRAC6, vous pouvez consulter les informations affichées dans l'écran **Surveillance de l'alimentation**.

---

## Inventaire de l'alimentation, bilan de puissance et plafonnement

Sur le plan de l'utilisation, vous pouvez ne disposer que d'un refroidissement limité au niveau du rack. Avec un plafond d'alimentation défini par l'utilisateur, vous pouvez allouer l'alimentation conformément aux besoins pour obtenir les performances requises.

iDRAC6 surveille la consommation électrique et limite dynamiquement les processeurs en fonction du plafond d'alimentation que vous avez défini afin d'optimiser les performances tout en répondant à vos exigences en matière d'alimentation.

---

## Surveillance de l'alimentation

iDRAC6 surveille continuellement la consommation électrique dans les serveurs PowerEdge. iDRAC6 calcule les valeurs d'alimentation suivantes et fournit les informations via son interface Web ou la CLI RACADM :

- Consommation électrique cumulée
- Consommation d'alimentation moyenne, minimale et maximale
- Valeurs de hauteur d'alimentation
- Consommation électrique (également affichée sous forme de graphiques dans l'interface Web)

---

## Configuration et gestion de l'alimentation

Vous pouvez utiliser l'interface Web iDRAC6 et l'interface de ligne de commande (CLI) de la RACADM pour gérer et configurer les commandes d'alimentation du système PowerEdge. Vous pouvez notamment :

- afficher la condition d'alimentation du serveur,
- exécuter des opérations de contrôle de l'alimentation sur le serveur (par exemple, mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation),
- afficher les informations du bilan de puissance du serveur et des blocs d'alimentation installés, notamment la consommation électrique potentielle minimale et maximale,
- afficher et configurer le seuil du bilan de puissance du serveur,

---

## Affichage de la condition d'intégrité des blocs d'alimentation.

La page **Blocs d'alimentation** indique la condition et la puissance des blocs d'alimentation installés dans le serveur.

## Utilisation de l'interface Web

Pour afficher la condition d'intégrité des blocs d'alimentation :

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Sélectionnez **Blocs d'alimentation** dans l'arborescence du système. La page **Blocs d'alimentation** affiche et fournit les informations suivantes :
   - **Condition de la redondance des blocs d'alimentation** : les valeurs possibles sont les suivantes :
   - **Totale :** les blocs d'alimentation PS1 et PS2 sont du même type et fonctionnent correctement.
   - **Perdue :** les blocs d'alimentation PS1 et PS2 sont de type différent ou l'un des deux ne fonctionne pas correctement. Aucune redondance n'existe.
   - **Désactivée :** un seul des deux blocs d'alimentation est disponible. Aucune redondance n'existe.
   - **Éléments des blocs d'alimentation individuels** : les valeurs possibles sont les suivantes :
   - **Condition** indique :
     - **OK** signifie que le bloc d'alimentation est présent et communique avec le serveur.
     - **Avertissement** signifie que seules des alertes d'avertissement ont été émises et qu'une action corrective doit être prise par l'administrateur. Si aucune action corrective n'est prise, des pannes d'alimentation critiques ou graves susceptibles d'affecter l'intégrité du serveur pourraient se produire.
     - **Grave** indique qu'au moins une alerte de panne a été émise. Une condition de panne indique une panne d'alimentation sur le serveur et la nécessité d'actions correctives immédiates.
   - **Emplacement** indique le nom du bloc d'alimentation : PS-n, n étant le numéro du bloc d'alimentation.
   - **Type** indique le type de bloc d'alimentation, tel que CA ou CC (conversion de tension CA-CC ou CC-CC).
   - **Puissance d'entrée** indique la puissance d'entrée du bloc d'alimentation, c'est-à-dire la charge d'alimentation CA maximale que le système peut faire supporter au centre de données.
   - **Puissance maximale** indique la puissance maximale du bloc d'alimentation, c'est-à-dire la puissance CC disponible pour le système. Cette valeur permet de confirmer qu'une capacité de bloc d'alimentation suffisante est disponible pour la configuration du système.
   - **Condition en ligne** indique l'état des blocs d'alimentation : présent et OK, entrée perdue, absent ou panne prévisible.
   - **Version ML** indique la version de micrologiciel du bloc d'alimentation.

**REMARQUE :** La puissance maximale diffère de la puissance d'entrée selon l'efficacité du bloc d'alimentation. Par exemple, si l'efficacité du bloc d'alimentation est de 89 % et la puissance maximale de 717 W, la puissance d'entrée est estimée à 797 W.

## Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

---

# Affichage du bilan de puissance

Le serveur fournit des aperçus de la condition du bilan de puissance du sous-système d'alimentation sur la page **Informations du bilan de puissance**.

## Utilisation de l'interface Web

**REMARQUE :** Vous devez disposer du privilège **Administrateur** pour effectuer des tâches de gestion de l'alimentation.

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Gestion de l'alimentation**.
3. Sélectionnez l'option **Bilan de puissance**.
4. La page **Informations du bilan de puissance** s'affiche.

Le premier tableau indique les limites minimale et maximale des seuils d'alimentation définis par l'utilisateur pour la configuration système en cours. Elles représentent la plage des consommations CA que vous pouvez définir comme plafond système. Une fois sélectionné, ce plafond constitue la charge d'alimentation CA maximale que le système peut faire supporter au centre de données.

**Consommation électrique potentielle minimale** représente la valeur Seuil du bilan de puissance la plus basse que vous puissiez définir.

**Consommation électrique potentielle maximale** représente la valeur Seuil du bilan de puissance la plus élevée que vous puissiez définir. Cette valeur

correspond également à la consommation électrique maximale absolue de la configuration système actuelle.

### Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

**REMARQUE :** Pour plus d'informations concernant cfgServerPower, y compris le détail des résultats renvoyés, consultez « cfgServerPower ».

---

## Seuil du bilan de puissance

Le seuil du bilan de puissance, s'il est activé, permet de définir une limite de plafonnement de l'alimentation pour le système. Les performances du système sont dynamiquement ajustées afin de maintenir la consommation électrique à proximité du seuil spécifié. La consommation électrique réelle peut être inférieure pour les faibles charges de travail et peut momentanément excéder le seuil jusqu'à ce que les ajustements de performances soient terminés.

Si vous cochez **Activé** pour Seuil du bilan de puissance, le système applique le seuil spécifié par l'utilisateur. Si vous laissez la valeur Seuil du bilan de puissance **non cochée**, le système n'est pas plafonné en alimentation. Par exemple, pour une configuration système donnée, la consommation de puissance électrique potentielle maximale est de 700 W et la consommation électrique potentielle minimale est de 500 W. Vous pouvez spécifier et activer un seuil du bilan de puissance pour ramener la consommation actuelle de 650 W à 525 W. Par la suite, les performances du système seront dynamiquement ajustées afin que la consommation électrique ne dépasse pas le seuil de 525 W spécifié par l'utilisateur.

### Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Gestion de l'alimentation**.
3. Sélectionnez l'option **Bilan de puissance**. La page **Informations du bilan de puissance** s'affiche.
4. Saisissez une valeur en watts, BTU/h ou pourcentage dans le tableau **Seuil du bilan de puissance**. La valeur spécifiée en watts ou BTU/h est la valeur limite du seuil du bilan de puissance. Si vous spécifiez une valeur en pourcentage, il s'agit d'un pourcentage de l'intervalle de la consommation électrique potentielle minimale-maximale. Par exemple, un seuil de 100 % signifie une consommation électrique potentielle maximale tandis que 0 % signifie une consommation électrique potentielle minimale.

   **REMARQUE :** Le seuil du bilan de puissance ne peut pas être supérieur à la consommation électrique potentielle maximale, ni inférieur à la consommation électrique potentielle minimale.

5. Cochez **Activé** pour activer le seuil ou laissez non coché. Si vous spécifiez **Activé**, le système applique le seuil spécifié par l'utilisateur. Si vous laissez l'option **non cochée**, le système n'est pas plafonné en alimentation.
6. Cliquez sur **Appliquer les modifications**.

### Utilisation de la RACADM

```
racadm config -g cfgServerPower -o cfgServerPowerCapWatts <valeur du plafond d'alimentation en watts>

racadm config -g cfgServerPower -o cfgServerPowerCapBTUhr <valeur du plafond d'alimentation en BTU/h>

racadm config -g cfgServerPower -o - cfgServerPowerCapPercent <valeur du plafond d'alimentation en %>
```

**REMARQUE :** Lors de la définition du seuil du bilan de puissance en BTU/h, la conversion en watts est arrondie à la valeur entière la plus proche. Lors de la relecture du seuil du bilan de puissance, la conversion de watts en BTU/h est de nouveau arrondie de cette manière. En conséquence, la valeur inscrite peut être nominalement différente de la valeur lue ; par exemple, un seuil défini sur 600 BTU/h sera relu avec la valeur 601 BTU/h.

---

## Affichage de la surveillance de l'alimentation

### Utilisation de l'interface Web

Pour afficher les données de surveillance de l'alimentation :

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Sélectionnez **Surveillance de l'alimentation** dans l'arborescence du système. La page **Surveillance de l'alimentation** s'affiche.

Les informations affichées sur la page **Surveillance de l'alimentation** sont décrites ci-après :

### Surveillance de l'alimentation

- **Condition : OK** indique que les blocs d'alimentation sont présents et communiquent avec le serveur, **Avertissement** indique qu'une alerte d'avertissement a été émise et **Grave** indique qu'une alerte de panne a été émise.
- **Nom de la sonde :** niveau du système de la carte système. Cette description indique que la sonde est surveillée par son emplacement dans le système.
- **Lecture :** la consommation électrique actuelle en watts/BTU/h.

### Intensité du courant

- **Emplacement :** indique le nom du bloc d'alimentation : PS-n, n étant le numéro du bloc d'alimentation.
- **Lecture :** la consommation électrique actuelle en ampères

### Statistiques de consommation de puissance

- **Consommation énergétique** affiche la consommation énergétique cumulée actuelle du serveur, mesurée à l'entrée des blocs d'alimentation. La valeur est indiquée en KWh et est une valeur cumulée qui représente l'énergie totale utilisée par le système. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser**.
- **Puissance système maximale** spécifie la valeur de puissance maximale dans l'intervalle spécifié par les heures de consommation initiale et maximale. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser**.
- **Intensité système maximale** spécifie la valeur de puissance maximale dans l'intervalle spécifié par les heures de consommation initiale et maximale. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser.**
- **Heure de début des mesures** affiche la date et l'heure enregistrées depuis que la dernière statistique a été effacée et qu'un nouveau cycle de mesures a débuté. Pour **Consommation énergétique**, vous pouvez réinitialiser la valeur avec le bouton **Réinitialiser**, mais elle persistera jusqu'à une opération de réinitialisation ou de basculement du système. Pour **Puissance système maximale** et **Intensité système maximale**, vous pouvez réinitialiser la valeur avec le bouton **Réinitialiser**, mais elle persistera également jusqu'à une opération de réinitialisation ou de basculement du système.
- **Heure de fin des mesures** affiche la date et l'heure de calcul de la consommation d'énergie du système pour l'affichage. **Heure de consommation maximale** affiche l'heure à laquelle la consommation maximale a été enregistrée.

**REMARQUE :** Les statistiques de consommation de puissance sont conservées lors des réinitialisations du système et reflètent ainsi l'ensemble des activités qui se sont produites dans l'intervalle entre les heures de début et de fin indiquées. Le bouton **Réinitialiser** permet de réinitialiser le champ respectif sur la valeur zéro. Dans le tableau suivant, les données de consommation électrique ne sont pas conservées lors des réinitialisations du système et sont alors ramenées à la valeur zéro. Les valeurs d'alimentation affichées sont des moyennes cumulées au cours de l'intervalle de temps respectif (minute, heure, jour et semaine précédents). Comme les intervalles de temps du début à la fin peuvent ici différer de ceux des statistiques de consommation de puissance, les valeurs d'alimentation maximales (maximum en watts par rapport à la consommation électrique maximale) peuvent différer.

### Consommation électrique

- Affiche la consommation électrique moyenne, maximale et minimale du système au cours de la minute, de l'heure, du jour et de la semaine précédents.
- Consommation électrique moyenne : moyenne de la minute précédente, heure précédente, jour précédent et semaine précédente.
- Consommation électrique maximale et consommation électrique minimale : les consommations électriques maximale et minimale observées au cours de l'intervalle de temps donné.
- Heure d'alimentation maximale et minimale : heure à laquelle les consommations électriques maximale et minimale ont été observées.

### Hauteur

**La hauteur instantanée du système** indique la différence entre l'alimentation disponible dans les blocs d'alimentation et la consommation électrique actuelle du système.

**La hauteur maximale du système** indique la différence entre l'alimentation disponible dans les blocs d'alimentation et la consommation électrique maximale du système.

### Afficher le graphique

Cliquez sur ce bouton pour afficher des graphiques illustrant la consommation d'alimentation et de courant, respectivement en watts et en ampères, d'iDRAC6 au cours de la dernière heure. L'utilisateur peut consulter ces statistiques pour la semaine précédente à l'aide du menu déroulant proposé au-dessus des graphiques.

**REMARQUE :** Chaque point de données tracé sur les graphiques représente la moyenne des lectures sur une période de 5 minutes. Par conséquent, les graphiques peuvent ne pas refléter les brèves fluctuations d'alimentation électrique ou de courant.

---

## Exécution de tâches de contrôle de l'alimentation sur le serveur

**REMARQUE :** Pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège **Administrateur de contrôle du châssis**.

iDRAC6 vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance, par exemple un arrêt méthodique.

## Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Gestion de l'alimentation**. La page **Contrôle de l'alimentation** s'affiche.
3. Sélectionnez l'une des **opérations de contrôle de l'alimentation** suivantes en cliquant sur le bouton radio correspondant :
   - **Mise sous tension du système** permet de mettre le serveur sous tension (équivaut à appuyer sur le bouton d'alimentation quand le serveur est hors tension). Cette option est désactivée si le système est déjà sous tension.
   - **Mise hors tension du système** permet d'éteindre le serveur. Cette option est désactivée si le système est déjà hors tension.
   - **NMI (Interruption non masquable)** génère une NMI pour arrêter le système.
   - **Arrêt normal** arrête le système.
   - **Réinitialisation du système (démarrage à chaud)** réinitialise le système sans le mettre hors tension. Cette option est désactivée si le système est déjà hors tension.
   - **Exécuter un cycle d'alimentation sur le système (démarrage à froid)** arrête, puis redémarre le système. Cette option est désactivée si le système est déjà hors tension.
4. Cliquez sur **Appliquer**. Une boîte de dialogue de confirmation s'affiche.
5. Cliquez sur **OK** pour effectuer la tâche de gestion de l'alimentation sélectionnée (réinitialisation du système, par exemple).

## Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur le serveur, ouvrez une session et tapez :

```
racadm serveraction <action>
```

où `<action>` a pour valeur powerup (mise sous tension), powerdown (mise hors tension), powercycle (cycle d'alimentation), hardreset (réinitialisation matérielle) ou powerstatus (condition de l'alimentation).

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration des fonctionnalités de sécurité

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



iDRAC6 dispose des fonctionnalités de sécurité suivantes :

- Options de sécurité avancée pour l'administrateur d'iDRAC6 :
  - L'option de désactivation de la redirection de console permet à l'utilisateur du système *local* de désactiver la redirection de console à l'aide de la fonctionnalité Redirection de console d'iDRAC6.
  - Les fonctionnalités de désactivation de la configuration locale permettent à l'administrateur d'iDRAC6 *distant* de désactiver de manière sélective la capacité de configuration d'iDRAC6 depuis les éléments suivants :
  - Option ROM du POST du BIOS
  - Système d'exploitation à l'aide de la RACADM locale et des utilitaires Dell™ OpenManage™ Server Administrator
- CLI RACADM et interface Web qui prennent en charge le cryptage SSL 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté)

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

- Configuration du délai d'expiration de la session (en secondes) via l'interface Web ou la CLI RACADM
- Ports IP configurables (si applicable)
- Secure Shell (SSH), qui utilise une couche de transport cryptée pour une sécurité plus élevée
- Limites d'échecs d'ouverture de session par adresse IP, avec blocage de l'ouverture de session à partir de l'adresse IP lorsque la limite est dépassée
- Plage d'adresses IP limitée pour les clients se connectant à iDRAC6

---

## Options de sécurité pour l'administrateur d'iDRAC6

### Désactivation de la configuration locale d'iDRAC6

Les administrateurs peuvent désactiver la configuration locale via l'interface utilisateur graphique (IUG) d'iDRAC6 en sélectionnant **Accès distant**→ **Réseau/Sécurité**→ **Services**. Lorsque la case à cocher **Désactiver la configuration locale d'iDRAC à l'aide de l'option ROM** est sélectionnée, l'utilitaire de configuration d'iDRAC6 (accessible en appuyant sur <Ctrl+E> lors du démarrage du système) fonctionne en mode Lecture seule, empêchant ainsi les utilisateurs locaux de configurer le périphérique. Lorsque l'administrateur sélectionne la case à cocher **Désactiver la configuration locale d'iDRAC à l'aide de la RACADM**, les utilisateurs locaux ne peuvent pas configurer iDRAC6 via l'utilitaire RACADM ou Dell OpenManage Server Administrator, bien qu'ils puissent toujours lire les paramètres de configuration.

Les administrateurs peuvent activer l'une de ces options ou les deux en même temps. En plus de les activer via l'interface Web, les administrateurs peuvent y parvenir à l'aide des commandes de la RACADM locale.

#### Désactivation de la configuration locale lors du redémarrage du système

Cette fonctionnalité désactive la capacité de l'utilisateur du système géré à configurer iDRAC6 pendant le redémarrage du système.

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

**REMARQUE :** Cette option n'est prise en charge que par l'utilitaire de configuration d'iDRAC6. Pour mettre à niveau vers cette version, mettez votre BIOS à niveau à l'aide du progiciel de mise à jour du BIOS disponible sur le site Web du support de Dell à l'adresse **support.dell.com**.

#### Désactivation de la configuration locale depuis la RACADM locale

Cette fonctionnalité désactive la capacité de l'utilisateur du système géré à configurer iDRAC6 à l'aide de la RACADM locale ou des utilitaires de Dell OpenManage Server Administrator.

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

**PRÉCAUTION : Ces fonctionnalités limitent considérablement la capacité de l'utilisateur local à configurer iDRAC6 depuis le système local, y compris la réinitialisation sur les valeurs par défaut de la configuration. Il est recommandé d'utiliser ces fonctionnalités comme bon vous semble. Désactivez uniquement une interface à la fois pour éviter de perdre les privilèges d'ouverture de session dans leur ensemble.**

**REMARQUE :** Consultez le livre blanc sur la *Désactivation de la configuration locale et du KVM virtuel distant dans DRAC* sur le site du support de Dell à l'adresse **support.dell.com** pour plus d'informations.

Bien que les administrateurs puissent définir les options de configuration locale à l'aide des commandes de la RACADM locale, ils peuvent les réinitialiser uniquement depuis une interface Web iDRAC6 hors bande ou une interface de ligne de commande pour des raisons de sécurité. L'option `cfgRacTuneLocalConfigDisable` s'applique une fois que l'auto-test de mise sous tension du système est terminé et que le système a démarré dans un environnement de système d'exploitation. Le système d'exploitation peut être un système d'exploitation Microsoft® Windows Server® ou Enterprise Linux capable d'exécuter des commandes de la RACADMlocale ou un système d'exploitation à usage limité tel que Microsoft Windows® Preinstallation Environment ou vmlinux servant à exécuter les commandes de la RACADM locale de Dell OpenManage Deployment Toolkit.

Plusieurs situations peuvent amener les administrateurs à désactiver la configuration locale. Par exemple, dans un centre de données ayant plusieurs administrateurs pour les serveurs et les périphériques d'accès distant, les administrateurs chargés de maintenir les piles de logiciels de serveurs peuvent ne pas avoir besoin d'un accès administratif aux périphériques d'accès distant. De même, les techniciens peuvent disposer d'un accès physique aux serveurs lors de la maintenance de routine des systèmes (au cours de laquelle ils peuvent redémarrer les systèmes et accéder au BIOS protégé par mot de passe), mais ils ne doivent pas être en mesure de configurer des périphériques d'accès distant. Dans de telles situations, les administrateurs des périphériques d'accès distant peuvent vouloir désactiver la configuration locale.

Les administrateurs doivent garder à l'esprit que, comme la désactivation de la configuration locale limite considérablement les privilèges de configuration locale, y compris la capacité à réinitialiser iDRAC6 sur sa configuration par défaut, ils doivent uniquement utiliser ces options lorsque cela est nécessaire et ils doivent généralement désactiver une seule interface à la fois pour éviter de perdre entièrement les privilèges d'ouverture de session. Par exemple, si les administrateurs ont désactivé tous les utilisateurs iDRAC6 locaux et n'autorisent que les utilisateurs du service de répertoire Microsoft Active Directory® à ouvrir une session sur iDRAC6 et si l'infrastructure d'authentification d'Active Directory échoue par la suite, les administrateurs risquent de ne plus pouvoir ouvrir une session. De même, si les administrateurs ont désactivé toute la configuration locale et placent un iDRAC6 ayant une adresse IP statique sur un réseau comprenant déjà un serveur DHCP (protocole de configuration dynamique de l'hôte) et que le serveur DHCP attribue par la suite l'adresse IP d'iDRAC6 à un autre périphérique sur le réseau, le conflit qui en résulte risque de désactiver la connectivité hors bande du DRAC, obligeant les administrateurs à réinitialiser le micrologiciel sur ses paramètres par défaut via une connexion série.

## Désactivation du KVM virtuel distant d'iDRAC6

Les administrateurs peuvent désactiver de manière sélective le KVM distant d'iDRAC6, offrant ainsi un mécanisme sécurisé flexible permettant à un utilisateur local de travailler sur le système sans qu'un tiers ne voit les actions de l'utilisateur par le biais de la redirection de console. L'utilisation de cette fonctionnalité nécessite l'installation du logiciel Managed Node d'iDRAC sur le serveur. Les administrateurs peuvent désactiver le vKVM distant à l'aide de la commande suivante :

```
racadm LocalConRedirDisable 1
```

La commande LocalConRedirDisable désactive les fenêtres de la session vKVM distante existante lorsqu'elle est exécutée avec l'argument 1

Pour éviter qu'un utilisateur distant n'annule les paramètres de l'utilisateur local, cette commande est uniquement disponible pour la RACADM locale. Les administrateurs peuvent utiliser cette commande sur les systèmes d'exploitation prenant en charge la RACADM, notamment Microsoft Windows Server 2003 et SUSE Linux Enterprise Server 10. Cette commande persistant au fur et à mesure des redémarrages du système, les administrateurs doivent expressément l'annuler pour réactiver le vKVM distant. Ils peuvent le faire en utilisant l'argument 0 :

```
racadm LocalConRedirDisable 0
```

Plusieurs situations peuvent obliger à désactiver le vKVM distant d'iDRAC6. Par exemple, les administrateurs peuvent vouloir empêcher un utilisateur iDRAC6 distant d'afficher les paramètres du BIOS qu'ils configurent sur un système, auquel cas ils peuvent désactiver le vKVM distant lors du POST du système en utilisant la commande `LocalConRedirDisable`. Ils peuvent aussi vouloir renforcer la sécurité en désactivant automatiquement le vKVM distant chaque fois qu'un administrateur ouvre une session sur le système, ce qu'ils peuvent faire en exécutant la commande `LocalConRedirDisable` à partir des scripts d'ouverture de session de l'utilisateur.

**REMARQUE :** Consultez le livre blanc sur la *Désactivation de la configuration locale et du KVM virtuel distant dans DRAC* sur le site du support de Dell à l'adresse **support.dell.com** pour plus d'informations.

Pour plus d'informations sur les scripts d'ouverture de session, consultez **technet2,microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx.**

---

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

Cette sous-section fournit des informations sur les fonctionnalités de sécurité des données suivantes qui sont intégrées dans votre iDRAC6 :

- « Secure Sockets Layer (SSL) »
- « Requête de signature de certificat (RSC) »
- « Accès au menu principal SSL »
- « Génération d'une requête de signature de certificat »

## Secure Sockets Layer (SSL)

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

Un système activé SSL :

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

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

Le serveur Web d'iDRAC6 inclut un certificat numérique SSL Dell auto-signé (référence serveur). Pour garantir un haut niveau de sécurité sur Internet, remplacez le certificat SSL du serveur Web en envoyant une requête à iDRAC6 pour générer une nouvelle requête de signature de certificat (RSC).

## Requête de signature de certificat (RSC)

Une RSC est une requête numérique adressée à une autorité de certification (AC) pour un certificat de serveur sécurisé. Les certificats de serveur sécurisé protègent l'identité d'un système distant et assurent que les informations échangées avec le système distant ne peuvent être ni affichées, ni modifiées par d'autres. Pour assurer la sécurité de votre DRAC, il est vivement recommandé de générer une RSC, de l'envoyer à une AC et de téléverser le certificat renvoyé par l'AC.

Une AC est une entité commerciale reconnue dans l'industrie informatique comme répondant à des normes élevées de filtrage et d'identification fiables, ainsi qu'à d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'AC. Une fois que l'AC  a reçu votre RSC, elle examine et vérifie les informations contenues dans la RSC. Si le demandeur satisfait aux normes de sécurité de l'AC, celle-ci lui émet un certificat qui identifie le demandeur de manière unique pour les transactions réseau et Internet.

Une fois que l'AC approuve la RSC et vous envoie un certificat, vous devez le téléverser vers le micrologiciel iDRAC6. Les informations de la RSC stockés sur le micrologiciel iDRAC6 doivent correspondre aux informations contenues dans le certificat.

## Accès au menu principal SSL

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **SSL**.

Utilisez la page **Menu principal SSL** (consultez le tableau 23-1) pour générer une RSC, téléverser un certificat de serveur existant ou afficher un certificat de serveur existant. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6. Le tableau 23-2 décrit les boutons disponibles sur la page **SSL**.

**Tableau 23-1. Menu principal SSL**

| Champ | Description |
|---|---|
| **Générer une requête de signature de certificat (RSC)** | Cliquez sur **Suivant** pour ouvrir la page qui vous permet de générer une RSC à envoyer à une AC pour demander un certificat Web sécurisé. |
| **Téléverser un certificat de serveur** | Cliquez sur **Suivant** pour téléverser un certificat existant qui appartient à votre société et qu'elle utilise pour contrôler l'accès à iDRAC6.<br><br>**REMARQUE :** iDRAC6 accepte uniquement les certificats X509 encodés en base 64. Les certificats encodés DER ne sont pas acceptés. Téléversez un nouveau certificat pour remplacer le certificat par défaut que vous avez reçu avec votre iDRAC6. |
| **Afficher le certificat de serveur** | Cliquez sur **Suivant** pour afficher un certificat de serveur existant. |

**Tableau 23-2. Boutons du menu principal SSL**

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

## Génération d'une requête de signature de certificat

**REMARQUE :** Chaque RSC écrase la RSC qui se trouve déjà dans le micrologiciel. Avant qu'iDRAC puisse accepter votre RSC signée, la RSC figurant dans le micrologiciel doit correspondre au certificat renvoyé par l'AC.

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

   Le tableau 23-3 décrit les options de la page **Générer une requête de signature de certificat (RSC)**.
3. Cliquez sur **Générer** pour ouvrir ou enregistrer la RSC.
4. Cliquez sur le bouton approprié de la page **Générer une requête de signature de certificat (RSC)** pour continuer. Le tableau 23-4 décrit les boutons

disponibles sur la page **Générer une requête de signature de certificat (RSC)**.

**Tableau 23-3. Options de la page Générer une requête de signature de certificat (RSC)**

| Champ | Description |
|---|---|
| **Nom commun** | Nom exact à certifier (généralement le nom de domaine du serveur Web, par exemple **www.xyzcompany.com**). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les espaces et les points sont valides. |
| **Nom de l'organisation** | Nom associé à cette organisation (par exemple, Compagnie XYZ). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides. |
| **Service de l'organisation** | Nom associé au service de l'organisation, comme un département (par exemple, Groupe de l'entreprise). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides. |
| **Ville** | Ville ou autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Seuls les caractères alphanumériques et les espaces sont valides. Ne séparez pas les mots par des traits de soulignement ou d'autres caractères. |
| **Nom de l'état** | État ou province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Seuls les caractères alphanumériques et les espaces sont valides. N'utilisez pas d'abréviations. |
| **Code de pays** | Nom du pays où se trouve l'entité qui fait la demande de certification. Utilisez le menu déroulant pour sélectionner le pays. |
| **E-mail** | Adresse e-mail associée à la RSC. Vous pouvez taper l'adresse e-mail de votre société ou une adresse e-mail que vous voulez associer à la RSC. Ce champ est optionnel. |

**Tableau 23-4. Boutons de la page Générer une requête de signature de certificat (RSC)**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime la page **Générer une requête de signature de certificat (RSC)**. |
| **Actualiser** | Recharge la page **Générer une requête de signature de certificat (RSC)**. |
| **Retour au menu principal SSL** | Retourne à la page **Menu principal SSL**. |
| **Générer** | Génère une RSC. |

## Affichage d'un certificat de serveur

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

   Le tableau 23-5 décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

2. Cliquez sur le bouton approprié de la page **Afficher le certificat de serveur** pour continuer.

**Tableau 23-5. Informations relatives au certificat**

| Champ | Description |
|---|---|
| **Numéro de série** | Numéro de série du certificat |
| **Informations sur le sujet** | Attributs du certificat 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 |

---

# Utilisation de Secure Shell (SSH)

Pour des informations sur l'utilisation de SSH, consultez « Utilisation de Secure Shell (SSH) ».

---

# Configuration des services

**REMARQUE :** Pour modifier ces paramètres, vous devez avoir le droit **Configurer iDRAC**. De plus, l'utilitaire de ligne de commande de la RACADM distante peut être activé uniquement si l'utilisateur a ouvert une session en tant que **root**.

1. Développez **l'arborescence** du Système et cliquez sur **Accès distant**.

2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Services**.

3. Configurez les services suivants, si nécessaire :
   - Configuration locale (tableau 23-6)
   - Serveur Web (tableau 23-7)
   - SSH (tableau 23-8)
   - Telnet (tableau 23-9)
   - RACADM distante (tableau 23-10)
   - Agent SNMP (tableau 23-11)
   - Agent de récupération de système automatique (tableau 23-12)

   Utilisez l'**agent de récupération de système automatique** pour activer la fonctionnalité **Écran de la dernière panne** d'iDRAC6.

   **REMARQUE : Server Administrator** doit être installé avec sa fonctionnalité **Récupération automatique** activée en configurant **Action** sur **Redémarrer le système**, **Arrêter le système** ou **Exécuter un cycle d'alimentation sur le système** pour que l'**Écran de la dernière panne** fonctionne dans iDRAC6.

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

5. Cliquez sur le bouton approprié de la page **Services** pour continuer. Consultez le tableau 23-13.

**Tableau 23-6. Paramètres de configuration locale**

| Paramètre | Description |
|---|---|
| **Désactiver la configuration locale d'iDRAC avec l'option ROM** | Désactive la configuration locale d'iDRAC à l'aide de l'option ROM. L'option ROM vous invite à saisir le module de configuration en appuyant sur <Ctrl+E> pendant le redémarrage du système. |
| **Désactiver la configuration locale d'iDRAC avec la RACADM** | Désactive la configuration locale d'iDRAC à l'aide de la RACADM locale. |

**Tableau 23-7. Paramètres du serveur Web**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive le serveur Web. Coché = Activé ; décoché = Désactivé. |
| **Nombre maximal de sessions** | Nombre maximal de sessions simultanées autorisées pour ce système. |
| **Sessions actives** | Nombre de sessions actuelles sur le système, inférieur ou égal au **Nombre maximal de sessions**. |
| **Délai d'expiration** | 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 Délai d'expiration prennent immédiatement effet et mettent fin à la session d'interface Web en cours. Le serveur Web est également réinitialisé. Veuillez attendre quelques minutes avant d'ouvrir une nouvelle session d'interface Web. La plage du délai d'expiration est comprise entre 60 et 10 800 secondes. La valeur par défaut est de 1 800 secondes. |
| **Numéro de port HTTP** | Port utilisé par iDRAC qui écoute une connexion serveur. Le paramètre par défaut est **80**. |
| **Numéro de port HTTPS** | Port utilisé par iDRAC qui écoute une connexion serveur. Le paramètre par défaut est **443**. |

**Tableau 23-8. Paramètres SSH**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive SSH. Lorsqu'elle est cochée, la case indique que SSH est activé. |
| **Délai d'expiration** | Délai d'expiration en cas d'inactivité Secure Shell, en secondes. La plage du délai d'expiration est comprise entre 60 et 1 920 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La plage par défaut est **300**. |
| **Numéro de port** | Port sur lequel iDRAC6 écoute une connexion SSH. Le numéro de port par défaut est **22**. |

**Tableau 23-9. Paramètres Telnet**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive Telnet. Lorsque la case est cochée, Telnet est activé. |
| **Délai d'expiration** | Délai d'expiration en cas d'inactivité Telnet, en secondes. La plage du délai d'expiration est comprise entre 60 et 1 920 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. Le délai d'expiration par défaut est **300**. |
| **Numéro de port** | Port sur lequel iDRAC6 écoute une connexion Telnet. Le numéro de port par défaut est **23**. |

**Tableau 23-10. Paramètres de la RACADM distante**

| Paramètre | Description |
|---|---|
| **Activé** | Active/Désactive la RACADM distante. Lorsque la case est cochée, la RACADM distante est activée. |
| **Sessions actives** | Nombre de sessions en cours sur le système. |
| **Sessions actives** | Nombre de sessions en cours sur le système, inférieur ou égal au **Nombre maximal de sessions**. |

**Tableau 23-11. Paramètres de l'agent SNMP**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive l'agent SNMP. Coché = Activé ; décoché = Désactivé. |
| **Nom de communauté** | Nom de communauté qui contient l'adresse IP pour la destination de l'alerte SNMP. Le nom de communauté peut comporter jusqu'à 31 caractères non blancs. Le paramètre par défaut est **public**. |

**Tableau 23-12. Paramètre de l'agent de récupération de système automatique**

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

**Tableau 23-13. Boutons de la page Services**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime la page **Services**. |
| **Actualiser** | Actualise la page **Services**. |
| **Appliquer les modifications** | Applique les paramètres de la page **Services**. |

---

# Activation d'options de sécurité iDRAC6 supplémentaires

Pour empêcher tout accès non autorisé à votre système distant, iDRAC6 fournit les fonctionnalités suivantes :

- Filtrage des adresses IP (IPRange) : définit une plage spécifique d'adresses IP auxquelles peut accéder iDRAC6.
- Blocage des adresses IP : limite le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP spécifique

Ces fonctionnalités sont désactivées dans la configuration par défaut d'iDRAC6. Utilisez la sous-commande suivante ou l'interface Web pour activer ces fonctionnalités :

```
racadm config -g cfgRacTuning -o <nom_objet> <valeur>
```

De plus, utilisez ces fonctionnalités en association avec les valeurs de délai d'expiration de la session en cas d'inactivité appropriées et un plan de sécurité défini pour votre réseau.

Les sous-sections suivantes fournissent des informations supplémentaires sur ces fonctionnalités.

## Filtrage IP (IpRange)

Le filtrage des adresses IP (ou *contrôle de plage IP*) permet un accès à iDRAC6 uniquement à partir des clients ou des stations de gestion dont les adresses IP sont comprises dans une plage spécifique à l'utilisateur. Toutes les autres ouvertures de session sont refusées.

Le filtrage IP compare l'adresse IP d'une ouverture de session entrante à la plage d'adresses IP qui est spécifiée dans les propriétés **cfgRacTuning** suivantes :

- `cfgRacTuneIpRangeAddr`
- `cfgRacTuneIpRangeMask`

La propriété **cfgRacTuneIpRangeMask** est appliquée à la fois à l'adresse IP entrante et aux propriétés **cfgRacTuneIpRangeAddr**. Si les résultats des deux propriétés sont identiques, la demande d'ouverture de session entrante est autorisée à accéder à iDRAC6. Les ouvertures de session à partir d'adresses IP situées à l'extérieur de cette plage reçoivent une erreur.

L'ouverture de session a lieu si l'expression suivante est égale à zéro :

```
cfgRacTuneIpRangeMask & (<adresse_IP_entrante> ^ cfgRacTuneIpRangeAddr)
```

où & est l'opérateur de bits AND des quantités et ^ est l'opérateur de bits OR exclusif.

Consultez « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 » pour une liste complète des propriétés **cfgRacTuning**.

**Tableau 23-14. Propriétés de filtrage des adresses IP (IpRange)**

| Propriété | Description |
|---|---|
| **cfgRacTuneIpRangeEnable** | Active la fonctionnalité Contrôle de plage IP. |
| **cfgRacTuneIpRangeAddr** | Détermine le format binaire d'adresse IP accepté en fonction des 1 dans le masque de sous-réseau.<br><br>Cette propriété correspond à l'opérateur de bits AND avec **cfgRacTuneIpRangeMask** pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP comportant ce format binaire dans ses bits supérieurs est autorisée à établir une session iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échoueront. Les valeurs par défaut dans chaque propriété permettent à une plage d'adresses de 192.168.1.0 à 192.168.1.255 d'établir une session iDRAC6. |
| **cfgRacTuneIpRangeMask** | Définit les positions binaires significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur. |

## Activation du filtrage IP

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

Consultez « Utilisation de la RACADM à distance » pour plus d'informations sur la RACADM et les commandes RACADM.

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

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

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

Pour restreindre les ouvertures de session à un petit ensemble de quatre adresses IP adjacentes (par exemple, 192.168.0.212 à 192.168.0.215), sélectionnez tout, sauf les deux bits inférieurs dans le masque, comme illustré ci-dessous :

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 252.255.255.255
```

## Instructions concernant le filtrage IP

Observez les instructions suivantes lorsque vous activez le filtrage IP :

- Assurez-vous que **cfgRacTuneIpRangeMask** est configuré sous forme de masque de réseau, où les bits de plus fort poids sont des 1 (ce qui définit le sous-réseau dans le masque) avec une transition de tous les 0 dans les bits de niveau inférieur.
- Utilisez l'adresse de base de la plage de votre choix comme valeur pour **cfgRacTuneIpRangeAddr**. La valeur binaire de 32 bits de cette adresse doit avoir des zéros dans tous les bits de niveau inférieur où il y a des zéros dans le masque.

## Blocage IP

Le blocage IP détermine de manière dynamique à quel moment un nombre excessif d'échecs d'ouverture de session se produit à partir d'une adresse IP particulière et (bloque (ou empêche) l'adresse d'ouvrir une session sur iDRAC6 pendant une période présélectionnée.

Le paramètre Blocage IP utilise les fonctionnalités de groupe **cfgRacTuning** telles que :

- Le nombre d'échecs d'ouverture de session autorisés
- L'intervalle de temps en secondes au cours duquel ces échecs doivent se produire
- La durée en secondes pendant laquelle l'adresse IP « coupable » n'est pas autorisée à établir une session une fois que le nombre total d'échecs autorisés est dépassé

Comme les échecs d'ouverture de session s'accumulent à partir d'une adresse IP spécifique, ils sont « datés » par un compteur interne. Lorsque l'utilisateur ouvre une session avec succès, l'historique des échecs est effacé et le compteur interne est remis à zéro.

**REMARQUE :** Lorsque des tentatives d'ouverture de session sont refusées à partir de l'adresse IP client, certains clients SSH peuvent afficher le message suivant : ssh exchange identification: Connection closed by remote host (identification d'échange ssh : connexion fermée par l'hôte distant).

Consultez « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 » pour une liste complète des propriétés **cfgRacTuning**.

Le tableau 23-15 répertorie les paramètres définis par l'utilisateur.

**Tableau 23-15. Propriétés de restriction des nouvelles tentatives d'ouverture de session**

| Propriété | Définition |
|---|---|
| **cfgRacTuneIpBlkEnable** | Active la fonctionnalité Blocage IP.<br><br>Lorsque des échecs consécutifs (**cfgRacTuneIpBlkFailCount**) à partir d'une seule adresse IP sont rencontrés pendant une période de temps spécifique (**cfgRacTuneIpBlkFailWindow**), toutes les tentatives ultérieures d'établissement d'une session à partir de cette adresse sont rejetées pendant un certain temps (**cfgRacTuneIpBlkPenaltyTime**). |
| **cfgRacTuneIpBlkFailCount** | Définit le nombre d'échecs d'ouverture de session à partir d'une adresse IP avant que les tentatives d'ouverture de session ne soient rejetées. |
| **cfgRacTuneIpBlkFailWindow** | Intervalle de temps en secondes pendant lequel les échecs d'ouverture de session sont comptés. Lorsque le nombre d'échecs dépasse cette limite, le compteur est remis à zéro. |
| **cfgRacTuneIpBlkPenaltyTime** | Définit l'intervalle de temps en secondes au cours duquel toutes les tentatives d'ouverture de session à partir d'une adresse IP avec des échecs excessifs sont rejetées. |

### Activation du blocage IP

L'exemple suivant empêche une adresse IP client d'établir une session pendant cinq minutes si ce client a échoué à ses cinq tentatives d'ouverture de session en l'espace d'une minute.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

L'exemple suivant empêche plus de trois échecs de tentatives en l'espace d'une minute et empêche toute tentative d'ouverture de session supplémentaire pendant une heure.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

## Configuration des paramètres de sécurité réseau à l'aide de l'IUG iDRAC6

**REMARQUE :** Vous devez disposer du droit **Configurer iDRAC6** pour effectuer les étapes suivantes.

1. Dans l'arborescence du **Système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Réseau**.
3. Sur la page **Configuration réseau**, cliquez sur **Paramètres avancés**.
4. Sur la page **Sécurité réseau**, configurez les valeurs d'attribut, puis cliquez sur **Appliquer les modifications**.

   Le tableau 23-16 décrit les paramètres de la page **Sécurité réseau**.
5. Cliquez sur le bouton approprié de la page **Sécurité réseau** pour continuer. Consultez le tableau 23-17 pour une description des boutons de la page **Sécurité réseau**.

**Tableau 23-16. Paramètres de la page Sécurité réseau**

| Paramètres | Description |
|---|---|
| **Plage IP activée** | Active la fonctionnalité Contrôle de la plage IP, qui définit une plage d'adresses IP spécifique pouvant accéder à iDRAC6. |
| **Adresse de la plage IP** | Détermine le format binaire d'adresse IP accepté, en fonction des 1 dans le masque de sous-réseau. Cette valeur correspond à l'opérateur de bits AND avec le masque de sous-réseau de la plage IP pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP comportant ce format binaire dans ses bits supérieurs est autorisée à établir une session iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échoueront. Les valeurs par défaut dans chaque propriété permettent à une plage d'adresses de 192.168.1.0 à 192.168.1.255 d'établir une session iDRAC6. |
| **Masque de sous-réseau de la plage IP** | Définit les positions binaires significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau, où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur.<br><br>Par exemple, **255.255.255.0.** |
| **Blocage IP activé** | Active la fonctionnalité 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 présélectionnée. |

| | |
|---|---|
| **Nombre d'échecs avant blocage IP** | Définit le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP avant que les tentatives d'ouverture de session ne soient rejetées à partir de cette adresse. |
| **Plage d'échecs avant blocage IP** | Détermine la période en secondes pendant laquelle des échecs du nombre d'échecs avant blocage IP doivent se produire pour déclencher la période de pénalité avant blocage IP. |
| **Période de pénalité avant blocage IP** | Période en secondes pendant laquelle les tentatives d'ouverture de session à partir d'une adresse IP avec un nombre d'échecs excessif sont rejetées. |

**Tableau 23-17. Boutons de la page Sécurité réseau**

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

---

Retour à la page du sommaire

Retour à la page du sommaire

# Installation de base d'iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



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

---

## Avant de commencer

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

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

---

## Installation du matériel iDRAC6 Express/Enterprise

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

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

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

---

## Configuration de votre système pour utiliser un iDRAC6

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

Pour exécuter l'utilitaire de configuration d'iDRAC6 :

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

   Si votre système d'exploitation commence à se charger alors que vous n'avez pas encore appuyé sur <Ctrl><E>, laissez-le terminer, puis redémarrez votre système et réessayez.
3. Configurez le LOM.
   a. À l'aide des touches fléchées, sélectionnez **Paramètres LAN,** puis appuyez sur <Entrée>. La page **Sélection du NIC** est affichée.
   b. À l'aide des touches fléchées, sélectionnez l'un des modes NIC suivants :
      - **Dédié :** sélectionnez cette option pour permettre au périphérique d'accès à distance d'utiliser l'interface réseau dédiée disponible sur iDRAC Enterprise. Cette interface n'est pas partagée avec le système d'exploitation hôte et achemine le trafic de gestion vers un réseau physique séparé en le séparant du trafic d'application Cette option est disponible uniquement si iDRAC6 Enterprise est installé dans le système. Après avoir installé la carte iDRAC6 Enterprise, assurez-vous de remplacer **Sélection du NIC** par **Dédié**. Cette opération peut être effectuée via l'utilitaire de configuration d'iDRAC6, l'interface Web iDRAC6 ou la RACADM.
      - **Partagé :** sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via le NIC 1 et le NIC 2, mais transmet des données seulement via le NIC 1. Si le NIC 1 est défectueux, le périphérique d'accès à distance n'est pas accessible.
      - **Partagé avec basculement LOM2 :** sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via le NIC 1 et le NIC 2, mais transmet des données seulement via le NIC 1. Si le NIC 1 échoue, le périphérique d'accès à distance bascule sur le NIC 2 pour l'intégralité de la transmission des données. Le périphérique d'accès à distance continue d'utiliser le NIC 2 pour la transmission des données. Si le NIC 2 échoue, le périphérique d'accès à distance rebascule toutes les transmissions de données sur le NIC 1 si l'échec du NIC 1 a été corrigé.
      - **Partagé avec basculement Tous les LOM :** sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via les NIC 1, NIC 2, NIC 3 et NIC 4, mais transmet des données seulement via le NIC 1. Si le NIC 1 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des

données sur le NIC 2. Si le NIC 2 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des données sur le NIC 3. Si le NIC 3 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des données sur le NIC 4. Si le NIC 4 échoue, le périphérique d'accès à distance rebascule l'intégralité de la transmission des données sur le NIC 1, mais uniquement si l'échec initial du NIC 1 a été corrigé. Il se peut que cette option ne soit pas disponible sur iDRAC6 Enterprise.

4. Configurez les paramètres LAN du contrôleur réseau pour utiliser DHCP ou une source d'adresse IP statique.
   a. À l'aide de la touche fléchée vers le bas, sélectionnez **Paramètres LAN**, puis appuyez sur <Entrée>.
   b. À l'aide des touches fléchées vers la gauche et vers la droite, sélectionnez **Source d'adresse IP**.
   c. À l'aide des touches fléchées vers la gauche et vers la droite, sélectionnez **DHCP, Auto Config** ou **Statique**.
   d. Si vous avez sélectionné **Statique**, configurez les paramètres **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut**.
   e. Appuyez sur <Échap>.
5. Appuyez sur <Échap>.
6. Sélectionnez **Enregistrer les modifications et quitter**.

---

# Présentation générale de l'installation et de la configuration du logiciel

Cette section donne une vue d'ensemble de haut niveau des procédures d'installation et de configuration du logiciel iDRAC6. Pour plus d'informations sur les composants du logiciel iDRAC6, consultez « Installation du logiciel sur le système géré ».

## Installation de votre logiciel iDRAC6

Pour installer votre logiciel iDRAC6 :

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

## Configuration de votre iDRAC6

Pour configurer votre iDRAC6 :

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

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

---

# Installation du logiciel sur le système géré

L'installation du logiciel sur le système géré est facultative. Sans le logiciel Managed System, vous ne pouvez pas utiliser la RACADM localement et iDRAC6 ne peut pas saisir l'écran de la dernière panne.

Pour installer le logiciel Managed System, installez le logiciel sur le système géré à l'aide du DVD *Dell Systems Management Tools and Documentation*.
Pour obtenir des instructions relatives à l'installation de ce logiciel, consultez votre *Guide d'installation rapide du logiciel* disponible sur le site Web du support de Dell à l'adresse **support.dell.com\manuals**.

Le logiciel Managed System installe vos choix à partir de la version appropriée de Dell™ OpenManage™ Server Administrator sur le système géré.

**REMARQUE :** N'installez pas les logiciels iDRAC6 Management Station Software et iDRAC6 Managed System Software sur le même système.

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

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

---

# Installation du logiciel sur la station de gestion

Votre système est fourni avec le DVD *Dell Systems Management Tools and Documentation*. Ce DVD est composé des éléments suivants :

- Racine du DVD : contient Dell Systems Build and Update Utility, qui fournit des informations de configuration du serveur et d'installation du système
- SYSMGMT : contient les produits Systems Management Software, dont Dell OpenManage Server Administrator

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

## Installation et retrait de la RACADM sur une station de gestion Linux

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

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

## Installation de la RACADM

1. Ouvrez une session en tant que root sur le système sur lequel vous voulez installer les composants de la station de gestion.
2. Si nécessaire, montez le DVD *Dell Systems Management Tools and Documentation* à l'aide de la commande suivante ou d'une commande similaire :

   ```
   mount /media/cdrom
   ```

3. Naviguez vers le répertoire **/linux/rac** et exécutez la commande suivante :

   ```
   rpm -ivh *.rpm
   ```

Si vous avez besoin d'aide avec la commande RACADM, tapez **racadm help** après avoir émis les commandes précédentes.

## Désinstallation de la RACADM

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

```
rpm -e <nom_du_progiciel_racadm>
```

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

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

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

---

# Mise à jour du micrologiciel iDRAC6

Utilisez l'une des méthodes suivantes pour mettre votre micrologiciel iDRAC6 à jour.

- Interface Web (consultez « Mise à jour du micrologiciel iDRAC6 avec l'interface Web »)
- CLI RACADM (consultez « Mise à jour du micrologiciel iDRAC6 avec la RACADM »)
- Progiciels Dell Update Package (consultez « Mise à jour du micrologiciel iDRAC6 à l'aide des progiciels Dell Update Package pour les systèmes d'exploitation Windows et Linux pris en charge »)

## Avant de commencer

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

1. Installez et activez les pilotes IPMI et de nud géré appropriés.
2. Si votre système fonctionne sous un système d'exploitation Windows, activez et démarrez le service **Windows Management Instrumentation** (WMI).
3. Si vous utilisez iDRAC6 Enterprise et que votre système exécute SUSE® Linux Enterprise Server (version 10) pour Intel® EM64T, démarrez le service **Raw.**
4. Débranchez et démontez le média virtuel.

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

5. Assurez-vous qu'USB est activé.

## Téléchargement du micrologiciel iDRAC6

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

Le progiciel de votre micrologiciel iDRAC6 se compose des éléments logiciels suivants :

- Code compilé et données du micrologiciel iDRAC6
- Fichiers de données de l'interface Web, JPEG et autres fichiers de données de l'interface utilisateur
- Fichiers de configuration par défaut

## Mise à jour du micrologiciel iDRAC6 avec l'interface Web

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

## Mise à jour du micrologiciel iDRAC6 avec la RACADM

Vous pouvez mettre à jour le micrologiciel iDRAC6 à l'aide de l'outil RACADM CLI. Si vous avez installé Server Administrator sur le système géré, utilisez la RACADM locale pour mettre à jour le micrologiciel.

1. Téléchargez sur le système géré l'image de micrologiciel iDRAC6 depuis le site Web du support de Dell à l'adresse **support.dell.com**.

   Par exemple :

   ```
   C:\downloads\firmimg.d6
   ```

2. Exécutez la commande RACADM suivante :

   ```
   racadm fwupdate -pud c:\downloads\
   ```

   Vous pouvez également mettre à jour le micrologiciel à l'aide de la RACADM distante et d'un serveur TFTP.

   Par exemple :

   racadm -r <*adresse IP iDRAC6*> U <*nom d'utilisateur*> -p <*mot de passe*> fwupdate -p -u -d <*chemin*>

   où *chemin* est l'emplacement sur le serveur TFTP où **firmimg.d6** est stocké.

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

Téléchargez et exécutez les progiciels Dell Update Package pour les systèmes d'exploitation Windows et Linux pris en charge depuis le site Web du support de Dell à l'adresse **support.dell.com**. Pour plus d'informations, reportez-vous au *Guide d'utilisation des progiciels Dell Update Package* disponible sur le site Web du support de Dell à l'adresse **support.dell.com / manuals**.

**REMARQUE :** Lors de la mise à jour du micrologiciel iDRAC6 à l'aide de l'utilitaire Dell Update Package dans Linux, les messages suivants peuvent s'afficher sur la console :

```
usb 5-2: device descriptor read/64, error -71
```

```
usb 5-2: device descriptor not accepting address 2, error -71
```

Ces erreurs sont superficielles et doivent être ignorées. Ces messages sont dus à la réinitialisation des périphériques USB au cours de la mise à jour du micrologiciel et sont inoffensifs.

## Effacement de la mémoire cache du navigateur

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

Pour plus d'informations, consultez « Effacer la mémoire cache de votre navigateur ».

---

# Configuration d'un navigateur Web pris en charge

Les sections suivantes donnent des instructions pour configurer les navigateurs Web pris en charge.

## Configuration de votre navigateur Web pour la connexion à l'interface Web iDRAC6

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

Pour configurer votre navigateur Web Internet Explorer pour accéder à un serveur proxy :

1. Ouvrez une fenêtre de navigateur Web.
2. Cliquez sur **Outils**, puis sur **Options Internet**.
3. Dans la fenêtre **Options Internet**, cliquez sur l'onglet **Connexions**.
4. Sous **Paramètres du réseau local (LAN)**, cliquez sur **Paramètres du LAN**.
5. Si la case **Utiliser un serveur proxy** est sélectionnée, sélectionnez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.
6. Cliquez sur **OK** deux fois.

## Liste des domaines de confiance

Lorsque vous accédez à l'interface Web 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 rétablir une connexion avec l'interface Web iDRAC6.

## Navigateurs Web 32 bits et 64 bits

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

## Affichage de versions localisées de l'interface Web

### Windows

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

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

Pour afficher une version localisée de l'interface Web iDRAC6 dans Internet Explorer :

1. Cliquez sur le menu **Outils** et sélectionnez **Options Internet**.

2. Dans la fenêtre **Options Internet**, cliquez sur **Langues**.
3. Dans la **fenêtre Langues**, cliquez sur **Ajouter**.
4. Dans la fenêtre **Ajouter une langue**, sélectionnez une langue prise en charge.

   Pour sélectionner plusieurs langues, appuyez sur <Ctrl>.
5. Sélectionnez la langue de votre choix et cliquez sur **Monter** pour déplacer la langue en haut de la liste.
6. Cliquez sur **OK**.
7. Dans la fenêtre **Langues**, cliquez sur **OK**.

## Linux

Si vous exécutez la redirection de console sur un client Red Hat® Enterprise Linux® (version 4) avec une IUG en chinois simplifié, le menu et le titre du visualiseur peuvent apparaître sous forme de caractères aléatoires. Ce problème est dû à l'encodage incorrect dans le système d'exploitation Red Hat Enterprise Linux (version 4) en chinois simplifié. Pour corriger ce problème, accédez et modifiez les paramètres d'encodage actuels en procédant comme suit :

1. Ouvrez un terminal de commande.
2. Tapez « paramètres régionaux » et appuyez sur <Entrée>. La sortie suivante s'affiche.

   ```
   LANG=zh_CN.UTF-8
   LC_CTYPE="zh_CN.UTF-8"
   LC_NUMERIC="zh_CN.UTF-8"
   LC_TIME="zh_CN.UTF-8"
   LC_COLLATE="zh_CN.UTF-8"
   LC_MONETARY="zh_CN.UTF-8"
   LC_MESSAGES="zh_CN.UTF-8"
   LC_PAPER="zh_CN.UTF-8"
   LC_NAME="zh_CN.UTF-8"
   LC_ADDRESS="zh_CN.UTF-8"
   LC_TELEPHONE="zh_CN.UTF-8"
   LC_MEASUREMENT="zh_CN.UTF-8"
   LC_IDENTIFICATION="zh_CN.UTF-8"
   LC_ALL=
   ```
3. Si les valeurs incluent "zh_CN.UTF-8", aucune modification n'est nécessaire. Si les valeurs n'incluent pas "zh_CN.UTF-8", passez à l'étape 4.
4. Naviguez vers le fichier **/etc/sysconfig/i18n**.
5. Dans le fichier, appliquez les modifications suivantes :

   Entrée actuelle :

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

   Entrée mise à jour :

   ```
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```
6. Fermez la session, puis ouvrez la session sur le système d'exploitation.
7. Relancez iDRAC6.

Lorsque vous passez de n'importe quelle autre langue au chinois simplifié, assurez-vous que ce problème n'existe plus. Sinon, répétez cette procédure.

Pour les configurations avancées d'iDRAC6, consultez « Configuration avancée d'iDRAC6 ».

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration d'iDRAC6 avec l'interface Web

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



iDRAC6 fournit une interface Web qui vous permet de configurer les propriétés et les utilisateurs d'iDRAC6, d'effectuer des tâches de gestion à distance et de dépanner un système distant (géré) en cas de problème. Pour la gestion quotidienne des systèmes, utilisez l'interface Web iDRAC6. Ce chapitre décrit comment effectuer les tâches de gestion de systèmes courantes en utilisant l'interface Web iDRAC6 et vous donne des liens vers des informations connexes.

La plupart des tâches de configuration de l'interface Web peuvent être exécutées à l'aide des commandes RACADM ou celles du protocole SM-CLP (Server Management-Command Line Protocol).

Les commandes de la RACADM locale sont exécutées à partir du serveur géré.

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

**PRÉCAUTION : Lorsque vous actualisez le navigateur en cliquant sur « Actualiser » ou en appuyant sur F5, il se peut que vous soyez déconnecté de la session d'IUG Web ou redirigé vers la page « Résumé du système ».**

---

## 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 accéder à l'interface Web à l'aide d'une adresse IPv4, passez à l'étape 2.

   Pour accéder à l'interface Web à l'aide d'une adresse IPv6, passez à l'étape 3.

2. Pour accéder à l'interface Web à l'aide d'une adresse IPv4, IPv4 doit être activé :

   Dans la barre **Adresse** du navigateur, tapez :

   `https://<adresse-IPv4-iDRAC>`

   Puis appuyez sur <Entrée>.

3. Pour accéder à l'interface Web à l'aide d'une adresse IPv6, IPv6 doit être activé.

   Dans la barre **Adresse** du navigateur, tapez :

   `https://[<adresse-IPv6-iDRAC>]`

   Puis appuyez sur <Entrée>.

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

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

   où *adresse-IP-iDRAC est l'adresse IP d'iDRAC6* et *numéro-de-port* le numéro de port HTTPS.

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

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

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

   où *adresse-IP-iDRAC* est l'adresse IP d'iDRAC6 et *numéro-de-port* le numéro de port HTTPS.

La fenêtre **Ouverture de session** iDRAC6 s'affiche.

## Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur iDRAC6 ou utilisateur Microsoft® Active Directory®. Le nom d'utilisateur et le mot de passe par défaut d'un utilisateur iDRAC6 sont **root** et **calvin**, respectivement.

Le privilège **Ouvrir une session sur iDRAC** doit vous avoir été octroyé par l'administrateur pour que vous puissiez ouvrir une session sur 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 des utilisateurs locaux est sensible à la casse. Les exemples sont `root`, `utilisateur_info` ou `john_doe`.
   - Votre nom d'utilisateur Active Directory.

     Les noms Active Directory peuvent être saisis sous la forme *<nom d'utilisateur>*, *<domaine>**<nom d'utilisateur>*, *<domaine>*/*<nom d'utilisateur>* ou *<utilisateur>*@*<domaine>*. Ils ne sont pas sensibles à la casse. Les exemples sont `dell.com\john_doe` ou `JOHN_DOE@DELL.COM`.
2. Dans le champ **Mot de passe**, tapez votre mot de passe utilisateur iDRAC6 ou Active Directory. Les mots de passe sont sensibles à la casse.
3. Depuis la boîte déroulante **Domaine**, sélectionnez *Cet iDRAC* pour ouvrir une session en tant qu'utilisateur iDRAC6 ou sélectionnez tout domaine disponible pour ouvrir une session en tant qu'utilisateur Active Directory.

   **REMARQUE :** Pour les utilisateurs Active Directory, si vous avez spécifié le nom du domaine comme faisant partie du nom d'utilisateur, sélectionnez *Cet iDRAC* dans le menu déroulant.
4. Cliquez sur **OK** ou appuyez sur <Entrée>.

## Fermeture de session

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

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

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

**REMARQUE :** La fermeture de l'interface Web iDRAC6 dans Microsoft Internet Explorer à l'aide du bouton Fermer (« x ») en haut à droite de la fenêtre peut générer une erreur d'application. Pour résoudre ce problème, téléchargez la dernière version de Cumulative Security Update for Internet Explorer à partir du site Web du support de Microsoft à l'adresse **support.microsoft.com**.

**PRÉCAUTION : Si vous avez ouvert plusieurs sessions d'IUG Web via <Ctrl+T> ou <Ctrl+N> pour accéder au même iDRAC6 à partir de la même station de gestion, puis fermez une de ces sessions, toutes les sessions d'IUG Web seront clôturées.**

## Utilisation des multiples onglets et fenêtres du navigateur

Des versions différentes de navigateurs Web font preuve de comportements différents à l'ouverture de nouveaux onglets et de nouvelles fenêtres. Microsoft Internet Explorer 6 ne prend pas en charge les onglets ; par conséquent, chaque fenêtre ouverte du navigateur devient une nouvelle session d'interface Web iDRAC6. Internet Explorer (IE) version 7 et IE 8 offrent la possibilité d'ouvrir des onglets ainsi que des fenêtres. Chaque onglet hérite des caractéristiques du dernier onglet ouvert. Appuyez sur `<Ctrl–T>` pour ouvrir un nouvel onglet et `<Ctrl–N>` pour ouvrir une nouvelle fenêtre de navigateur à partir de la session active. Vous serez connecté à l'aide de vos références déjà authentifiées. La fermeture d'un onglet, quel qu'il soit, fait expirer tous les onglets de l'interface Web iDRAC6. En outre, si un utilisateur ouvre une session avec des privilèges Utilisateur privilégié sur un onglet, puis qu'il ouvre une session en tant qu'administrateur sur un autre onglet, les deux onglets ouverts possèdent des privilèges Administrateur.

Le comportement des onglets dans Mozilla Firefox 2 et Firefox 3 est le même que dans IE 7 et IE 8 ; les nouveaux onglets correspondent à de nouvelles sessions. Les écrans lancés à l'aide du navigateur Firefox fonctionneront avec les mêmes privilèges que ceux de 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 Administrateur, **les deux** utilisateurs auront des privilèges Administrateur.

**Tableau 4-1. Comportement des privilèges utilisateur dans les navigateurs pris en charge**

| Navigateur | Comportement des onglets | Comportement des fenêtres |
|---|---|---|
| **Microsoft Internet Explorer 6** | Inapplicable | Nouvelle session |
| **Microsoft IE7 et IE8** | Depuis la dernière session ouverte | Nouvelle session |
| **Firefox 2 et Firefox 3** | 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. Consultez « Configuration de votre 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 droit **Configurer iDRAC** pour effectuer les étapes suivantes.

**REMARQUE :** La plupart des serveurs DHCP requièrent un serveur pour stocker un jeton d'identifiant 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 de client à l'aide d'un numéro (0) d'interface à un octet suivi par une adresse MAC à six octets.

**REMARQUE :** Si vous travaillez avec le protocole STP (Spanning Tree Protocol) activé, assurez d'activer également PortFast ou une technologie similaire comme suit :

- Sur les ports pour le commutateur connecté à iDRAC6
- Sur les ports connectés à la station de gestion exécutant une session KVM iDRAC

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

1. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**→ **Réseau.**
2. Sur la page **Réseau,** vous pouvez saisir les paramètres réseau, les paramètres courants d'iDRAC6, les paramètres IPv4, les paramètres IPv6, les paramètres IPMI et les paramètres VLAN. Consultez le tableau 4-2, le tableau 4-3, le tableau 4-4, le tableau 4-5, le tableau 4-6 et le tableau 4-7 pour les descriptions de ces paramètres.
3. Après avoir saisi les paramètres requis, cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 4-8.

**Tableau 4-2. Paramètres réseau**

| Paramètre | Description |
|---|---|
| **Sélection du NIC** | Configure le mode courant sur les quatre modes possibles :<br><br>· Dédié<br><br>**REMARQUE :** Cette option n'est disponible que sur les cartes iDRAC6 Enterprise.<br><br>· Partagé (LOM1)<br><br>· Partagé avec basculement LOM2<br><br>· Partagé avec basculement tous les LOM<br><br>**REMARQUE :** Il se peut que cette option ne soit pas disponible sur iDRAC6 Enterprise.<br><br>**REMARQUE :** iDRAC6 ne communique pas localement via le même port physique si **Sélection du NIC** est définie sur le mode **Partagé** ou **Partagé avec basculement**. Cela est dû au fait qu'un commutateur réseau n'envoie pas les paquets via le port par l'intermédiaire duquel il les a reçus. |
| **Adresse MAC** | Affiche l'adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nud d'un réseau. |
| **Activer le NIC** | Lorsqu'il est coché, ce paramètre indique que le NIC est activé et active les commandes restantes de ce groupe. Lorsqu'un NIC est désactivé, toutes les communications avec iDRAC6 via le réseau sont bloquées.<br><br>La valeur par défaut est **Activé**. |
| **Négociation automatique** | S'il est défini sur **Activé**, il affiche la vitesse du réseau et le mode en communiquant avec le routeur ou le concentrateur le plus proche. S'il est défini sur **Désactivé**, il vous permet de définir la vitesse du réseau et le mode duplex manuellement.<br><br>Si **Sélection du NIC** n'est *pas* défini sur **Dédié**, le paramètre Négociation automatique est toujours activée (**Activé)**. |
| **Vitesse du réseau** | Vous permet de définir la vitesse du réseau sur 100 Mbps ou 10 Mbps en fonction des besoins de votre environnement réseau. Cette option n'est pas disponible si Négociation automatique est défini sur **Activé**. |
| **Mode duplex** | Vous permet de définir le mode semi-duplex ou duplex intégral en fonction des besoins de votre environnement réseau. Cette option n'est pas disponible si **Négociation automatique** est défini sur **Activé**. |
| **MTU du NIC** | Vous permet de définir la taille MTU (Maximum Transmission Unit) sur le NIC. |

**Tableau 4-3. Paramètres communs**

| Paramètre | Description |
|---|---|
| **Enregistrer iDRAC sur DNS** | Enregistre le nom iDRAC6 sur le serveur DNS.<br><br>La valeur par défaut est **Désactivé**. |
| **Nom iDRAC DNS** | Affiche le nom iDRAC6 uniquement lorsque **Enregistrer iDRAC sur DNS** est sélectionné. 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. |
| **Nom de domaine Auto Config** | Utilise le nom de domaine DNS par défaut. Lorsque la case à cocher n'est pas sélectionnée et que l'option **Enregistrer iDRAC sur DNS** est sélectionnée, modifiez le nom de domaine DNS dans le champ **Nom de domaine DNS**.<br><br>La valeur par défaut est **Désactivé**. |
| **Nom de domaine DNS** | Le champ **Nom de domaine DNS** par défaut est vide. Lorsque la case à cocher **Nom de domaine Auto Config** est sélectionnée, cette option est désactivée. |

**Tableau 4-4. Paramètres IPv4**

| Paramètre | Description |
|---|---|
| **Activer IPv4** | Si le NIC est activé, celui-ci sélectionne la prise en charge du protocole IPv4 et définit les autres champs de cette section à activer. |
| **Activation DHCP** | Invite iDRAC6 à obtenir une adresse IP pour le NIC sur le serveur de protocole de configuration dynamique à l'hôte (DHCP). La valeur par défaut est **Désactivé**. |
| **Adresse IP** | Spécifie l'adresse IP du NIC iDRAC6. |
| **Masque de sous-réseau** | Vous permet de saisir ou de modifier une adresse IP statique pour le NIC iDRAC6. Pour modifier ce paramètre, désélectionnez la case à cocher Utiliser DHCP (pour l'adresse IP du NIC ). |
| **Passerelle** | Adresse d'un routeur ou d'un commutateur. La valeur est au format « séparé par un point », tel que 192.168.0.1. |
| **Utiliser DHCP pour obtenir des adresses de serveur DNS** | Activez DHCP pour obtenir des adresses de serveur DNS en sélectionnant la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Lorsque vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS préféré** et **Autre serveur DNS**.<br><br>La valeur par défaut est **Désactivé**.<br><br>**REMARQUE :** Lorsque la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS** est sélectionnée, les adresses IP ne peuvent pas être saisies dans les champs **Serveur DNS préféré** et **Autre serveur DNS**. |
| **Serveur DNS préféré** | Adresse IP du serveur DNS. |
| **Autre serveur DNS** | Autre adresse IP |

**Tableau 4-5. Paramètres IPv6**

| Paramètre | Description |
|---|---|
| **Activer IPv6** | Si la case à cocher est sélectionnée, IPv6 est activé. Si la case à cocher n'est pas sélectionnée, IPv6 est désactivé. La valeur par défaut est Désactivé. |
| **Activation de la configuration automatique** | Cochez cette case pour permettre à iDRAC6 d'obtenir l'adresse IPv6 du NIC iDRAC6 auprès du serveur de protocole de configuration dynamique à l'hôte (DHCPv6). En outre, l'activation de la configuration automatique désactive et supprime les valeurs statiques de l'adresse IP 1, de la longueur du préfixe et de la passerelle IP. |
| **Adresse IP 1** | Configure l'adresse IPv6 du NIC iDRAC. Pour modifier ce paramètre, vous devez tout d'abord désactiver **AutoConfig** en désélectionnant la case à cocher associée. |
| **Longueur du préfixe** | Configure la longueur du préfixe de l'adresse IPv6. Il peut s'agir de toute valeur comprise entre 1 et 128 compris. Pour modifier ce paramètre, vous devez tout d'abord désactiver **AutoConfig** en désélectionnant la case à cocher associée. |
| **Passerelle** | Configure la passerelle statique pour le NIC iDRAC. Pour modifier ce paramètre, vous devez tout d'abord désactiver **AutoConfig** en désélectionnant la case à cocher associée. |
| **Adresse locale de liaison** | Spécifie l'adresse IPv6 du NIC iDRAC6. |
| **Adresse IP 2...15** | Spécifie l'adresse IPv6 du NIC iDRAC6 supplémentaire en cas de disponibilité. |
| **Utiliser DHCP pour obtenir des adresses de serveur DNS** | Activez DHCP pour obtenir des adresses de serveur DNS en sélectionnant la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Lorsque vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS préféré** et **Autre serveur DNS**.<br><br>La valeur par défaut est Désactivé.<br><br>REMARQUE : Lorsque la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS** est sélectionnée, les adresses IP ne peuvent pas être saisies dans les champs **Serveur DNS préféré** et **Autre serveur DNS**. |
| **Serveur DNS préféré** | Configure l'adresse IPv6 statique du serveur DNS préféré. Pour modifier ce paramètre, vous devez tout d'abord décocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. |
| **Autre serveur DNS** | Configure l'adresse IPv6 statique de l'autre serveur DNS. Pour modifier ce paramètre, vous devez tout d'abord décocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. |

**Tableau 4-6. Paramètres IPMI**

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

**Tableau 4-7. Paramètres VLAN**

| Paramètre | Description |
|---|---|
| **Activer le n° VLAN** | Si cette option est activée, seul le trafic du numéro du LAN virtuel (VLAN) est accepté. |
| **N° VLAN** | Champ N° VLAN des champs 802.1g. Saisissez une valeur valide pour le numéro du VLAN (doit être un numéro entre 1 et 4 094). |
| **Priorité** | Champ Priorité des champs 802.1g. Saisissez un numéro entre 0 et 7 pour définir la priorité du numéro du VLAN. |

**Tableau 4-8. Boutons de la page Configuration réseau**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime les valeurs **Réseau** qui apparaissent à l'écran. |
| **Actualiser** | Recharge la page **Réseau**. |
| **Paramètres avancés** | Ouvre la page **Sécurité réseau** pour permettre à l'utilisateur de saisir les attributs Plage IP et Blocage IP. |
| **Appliquer** | Enregistre les nouveaux paramètres définis sur la page **Réseau**.<br><br>**REMARQUE :** Les modifications des paramètres de l'adresse IP du NIC ferment toutes les sessions utilisateur et forcent les utilisateurs à se reconnecter à l'interface Web d'iDRAC6 avec les paramètres d'adresse IP mis à jour. Toutes les autres modifications nécessitent la réinitialisation du NIC, qui peut provoquer une perte brève de connectivité. |

## Configuration du filtrage IP et du blocage IP

**REMARQUE :** Vous devez disposer du droit **Configurer iDRAC** pour effectuer les étapes suivantes.

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

   Le tableau 4-9 décrit les **paramètres de la page Sécurité réseau**. Une fois les paramètres configurés, cliquez sur **Appliquer**.
3. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 4-10.

**Tableau 4-9. Paramètres de la page Sécurité réseau**

| Paramètres | Description |
|---|---|
| **Plage IP activée** | Active la fonctionnalité Vérification de la plage IP, qui définit une plage d'adresses IP pouvant accéder à iDRAC. La valeur par défaut est **Désactivé**. |
| **Adresse de la plage IP** | Détermine le format binaire d'adresse IP acceptéen fonction des 1 dans le masque de sous-réseau. Cette valeur correspond à l'opérateur de bits AND avec le masque de sous-réseau de la plage IP pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP comportant ce format binaire dans ses bits supérieurs est autorisée à établir une session sur un iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échouent. Les valeurs par défaut dans chaque propriété permettent à une plage d'adresses de 192.168.1.0 à 192.168.1.255 d'établir une session sur iDRAC6. |
| **Masque de sous-réseau de la plage IP** | Définit les positions des bits significatifs dans l'adresse IP. Le masque de sous-réseau 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. L'adresse par défaut est **255.255.255.0**. |
| **Blocage IP activé** | Active la fonctionnalité 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 présélectionnée. 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 que les tentatives d'ouverture de session ne soient rejetées à partir de cette adresse. Le nombre 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. La période par défaut est **3 600**. |
| **Période de** | Période, en secondes, pendant laquelle les tentatives d'ouverture de session à partir d'une adresse IP avec un nombre d'échecs excessif |

| | |
|---|---|
| **pénalité avant blocage IP** | sont rejetées. La période par défaut est **3 600.** |

**Tableau 4-10. Boutons de la page Sécurité réseau**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime les valeurs **Sécurité réseau** qui apparaissent à l'écran. |
| **Actualiser** | Recharge la page **Sécurité réseau**. |
| **Appliquer** | Enregistre les nouveaux paramètres que vous avez créés dans la page **Sécurité réseau**. |
| **Retourn à la page Configuration réseau** | Retourne à la page **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 d'événements sur plateforme [PET] et/ou par e-mail).

Les événements sur plateforme filtrables sont répertoriés dans le tableau 4-11.

**Tableau 4-11. Filtres d'événements sur plateforme**

| Index | Événement sur plateforme |
|---|---|
| 1 | Assertion de ventilateur critique |
| 2 | Assertion d'avertissement concernant la batterie |
| 3 | Assertion critique de la batterie |
| 4 | Assertion critique de la tension discrète |
| 5 | Assertion d'avertissement concernant la température |
| 6 | Assertion critique de la température |
| 7 | Assertion critique d'intrusion |
| 8 | Redondance dégradée |
| 9 | Perte de la redondance |
| 10 | Assertion d'avertissement concernant le processeur |
| 11 | Assertion critique du processeur |
| 12 | Processeur absent |
| 13 | Assertion d'avertissement concernant le bloc d'alimentation |
| 14 | Assertion critique du bloc d'alimentation |
| 15 | Bloc d'alimentation absent |
| 16 | Assertion critique du journal des événements |
| 17 | Assertion critique de la surveillance |
| 18 | Assertion d'avertissement concernant l'alimentation système |
| 19 | Assertion critique de l'alimentation système |
| 20 | Assertion d'informations de la carte SD discrète |
| 21 | Assertion critique de la carte SD discrète |
| 22 | Assertion d'avertissement concernant la carte SD discrète |

Lorsqu'un événement sur plateforme se produit (par exemple, une assertion d'avertissement concernant la 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'événements sur plateforme est également configuré pour effectuer une action (tel qu'un redémarrage du système), l'action est effectuée.

## Configuration des filtres d'événements sur plateforme (PEF)

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

1. Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge. Consultez « Accès à l'interface Web ».
2. Cliquez sur **Système**→ **Gestion des alertes**→ **Événements sur plateforme**.

3. Dans le premier tableau, sélectionnez la case à cocher **Activer les alertes de filtre d'événements sur plateforme,** puis cliquez sur **Appliquer**.

   **REMARQUE : Activer les alertes de filtres d'événements sur plateforme** doit être activé pour qu'une alerte soit envoyée à une destination configurée valide (PET ou e-mail).

4. Dans le tableau suivant, **Liste des filtres d'événements sur plateforme**, cliquez sur le filtre à configurer.

5. À la page **Définir les événements sur plateforme**, sélectionnez l'action appropriée **Éteindre** ou sélectionnez **Aucun**.

6. Sélectionnez ou désélectionnez **Générer une alerte** pour activer ou désactiver cette action.

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

7. Cliquez sur **Appliquer**.

   Vous retournez à la page **Événements sur plateforme** où les modifications que vous avez appliquées sont affichées dans la **Liste des filtres d'événements sur plateforme.**

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

## Configuration des interruptions d'événement sur plateforme (PET)

**REMARQUE :** Vous devez disposer du droit **Configurer iDRAC** pour ajouter ou activer/désactiver une alerte SNMP. Les options suivantes ne sont pas disponibles si vous ne disposez pas du droit **Configurer iDRAC**.

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

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

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

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

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

6. Saisissez une adresse IP valide de destination d'interruption d'événement sur plateforme et cliquez sur **Appliquer**.

7. Cliquez sur **Envoyer l'interruption test** pour tester l'alerte configurée ou cliquez sur **Retour à la page Destination des alertes sur plateforme**.

   **REMARQUE :** Votre compte d'utilisateur doit avoir le droit **Alertes test** afin d'envoyer une interruption test. Consultez le tableau 6-6, « Droits de groupes iDRAC », pour de plus amples informations.

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

8. Dans le champ **Chaîne de la communauté**, saisissez le nom de la communauté SNMP iDRAC approprié. Cliquez sur **Appliquer**.

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

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

**REMARQUE :** Si vous désactivez un filtre d'événements sur plateforme, l'interruption associée à ce capteur « défaillant » est également désactivée. Les interruptions associées aux transitions « défaillantes vers fonctionnelles » sont toujours générées si l'option **Activer les alertes de filtres d'événements sur plateforme** est cochée ou activée. Par exemple, si vous désactivez l'option **Générer une alerte** pour le **Filtre d'assertion d'informations concernant la carte SD discrète** et retirez la carte SD, l'interruption associée n'est pas affichée. L'interruption est générée si vous insérez à nouveau la carte SD. En revanche, si vous activez le filtre d'événements sur plateforme, une interruption est générée lors du retrait et de l'insertion.

## Configuration des alertes par e-mail

**REMARQUE :** Les alertes par e-mail prennent en charge les adresses IPv4 et IPv6.

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

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

3. Cliquez sur **Système**→ **Gestion des alertes**→ **Paramètres d'alertes par e- mail**.

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

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

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

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

8. Cliquez sur **Appliquer**.

9. Si vous voulez tester l'alerte par e-mail configurée, cliquez sur **Envoyer un e-mail test**. Sinon, cliquez sur **Retour à la page Destination des alertes par e-mail**.

10. Cliquez sur **Retour à la page Destination des alertes par e-mail** et saisissez une adresse IP SMTP valide dans le champ **Adresse IP du serveur SMTP (e-mail).**

    **REMARQUE :** Pour envoyer un e-mail test avec succès, l'**adresse IP du serveur SMTP (e-mail)** doit être configurée sur la page **Paramètres des alertes par e-mail**. Le serveur SMTP utilise l'adresse IP définie pour communiquer avec iDRAC6 afin d'envoyer des alertes par e-mail lorsqu'un événement sur plateforme se produit.

11. Cliquez sur **Appliquer**.

12. Répétez les étapes 4 à 9 pour configurer des destinations d'alertes par e- mail supplémentaires.

## Configuration d'IPMI

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

2. Configurez IPMI sur LAN.

   a. Dans l'arborescence du **système**, cliquez sur **Accès distant**.

   b. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Réseau**.

   c. Sur la page **Réseau** sous **Paramètres IPMI**, sélectionnez **Activer IPMI sur LAN** et cliquez sur **Appliquer**.

   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 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+.

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

   **REMARQUE :** La clé de cryptage doit se composer d'un nombre pair de caractères hexadécimaux d'un maximum de 40 caractères.

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

   a. Dans l'arborescence du **système**, cliquez sur **Accès distant**.

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

   c. Sur la page **Communications série sur LAN**, sélectionnez **Activer les communications série sur LAN**.

   d. Mettez à jour le débit en bauds de SOL IPMI.

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

   e. Cliquez sur le menu déroulant **Débit en bauds**, sélectionnez le débit en bauds approprié et cliquez sur **Appliquer**.

   f. Mettez à jour le privilège requis minimal. Cette propriété définit le privilège utilisateur minimal qui est requis pour utiliser la fonctionnalité **Communications série sur LAN**.

Cliquez sur le menu déroulant **Limite du niveau de privilège du canal**, puis sélectionnez **Utilisateur**, **Opérateur** ou **Administrateur**.

g. Cliquez sur **Appliquer**.

4. Configurez les communications série IPMI.
   a. Dans l'onglet **Réseau/Sécurité**, cliquez sur **Série**.
   b. Dans le menu **Série**, remplacez le mode de connexion des communications série IPMI par le paramètre approprié.

      Sous **Communications série IPMI**, cliquez sur le menu déroulant **Paramètres du mode de connexion** et sélectionnez le mode approprié.

   c. Configurez le débit en bauds des communications série IPMI.

      Cliquez sur le menu déroulant **Débit en bauds**, sélectionnez le débit en bauds approprié et cliquez sur **Appliquer**.

   d. Définissez la **limite du niveau de privilège du canal** et le **contrôle du débit**.
   e. Cliquez sur **Appliquer**.
   f. Assurez-vous que MUX série est correctement défini dans le programme de configuration du BIOS du système géré.
      - Redémarrez votre système.
      - Pendant le POST, appuyez sur <F2> pour accéder au programme de configuration du BIOS.
      - Naviguez vers **Serial Communication (Communications série)**.
      - Dans le menu **Serial Connection (Connexion série)**, assurez-vous que **External Serial Connector (Connecteur série externe)** est défini sur **Remote Access Device (Périphérique d'accès à distance)**.
      - Enregistrez et quittez le programme de configuration du BIOS.
      - Redémarrez votre système.

Si les communications série IPMI sont en mode terminal, vous pouvez configurer les paramètres supplémentaires suivants :

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

Pour plus d'informations sur ces propriétés, consultez la spécification d'IPMI 2.0. Pour de plus amples informations sur les commandes en mode terminal, consultez le *Guide d'utilisation des utilitaires du contrôleur de gestion de la carte mère Dell OpenManage* à l'adresse **support.dell.com / manuals**.

---

## Configuration des utilisateurs d'iDRAC6

Consultez « Ajout et configuration d'utilisateurs iDRAC6 » pour obtenir des informations détaillées.

---

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

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

- Secure Sockets Layer (SSL)
- Requête de signature de certificat (RSC)
- Accès à SSL via l'interface Web
- Génération d'une RSC
- Téléversement d'un certificat de serveur
- Affichage d'un certificat de serveur

### Secure Sockets Layer (SSL)

iDRAC6 inclut un serveur Web qui est 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 par 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 activé SSL peut effectuer les tâches suivantes :

- S'authentifier sur un client activé 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, la forme la plus sécurisée 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 du serveur Web 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 (AC) telle que VeriSign ou Thawte.

## Requête de signature de certificat (RSC)

Une RSC est une requête numérique envoyée à une AC en vue d'obtenir un certificat de serveur sécurisé. Les certificats de serveur sécurisés permettent aux clients du serveur de faire confiance à l'identité du serveur auquel ils se sont connectés et de négocier une session cryptée avec le serveur.

Une autorité de certification est une entité commerciale reconnue dans l'industrie de l'informatique pour ses critères élevés en matière d'analyse et d'identification fiables et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'AC. Une fois que l'AC reçoit une RSC, elle la contrôle et vérifie les informations qu'elle contient. Si le postulant remplit les normes de sécurité de l'AC, cette dernière émet 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'AC approuve la RSC et envoie le certificat, téléversez ce dernier sur le micrologiciel iDRAC6. Les informations de la RSC stockées sur le micrologiciel iDRAC6 doivent correspondre aux informations du certificat.

## Accès à SSL via l'interface Web

1. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**.
2. Cliquez sur **SSL** pour ouvrir la page **SSL**.

Utilisez la page **SSL** pour effectuer l'une des options suivantes :

- Générer une requête de signature de certificat (RSC) à envoyer à une AC. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6.
- Téléverser un certificat de serveur.
- Afficher un certificat de serveur.

Le tableau 4-12 décrit les options de la page **SSL** ci-dessus.

**Tableau 4-12. Options de la page SSL**

| Champ | Description |
|---|---|
| **Générer une requête de signature de certificat (RSC)** | Cette option vous permet de générer une RSC à envoyer à une AC pour demander un certificat Web sécurisé.<br><br>**REMARQUE :** Chaque nouvelle RSC supplante celle qui se trouve déjà sur le micrologiciel. Pour qu'une AC accepte votre RSC, la RSC du micrologiciel doit correspondre au certificat renvoyé par l'AC. |
| **Téléverser le certificat de serveur** | Cette option vous permet de téléverser un certificat existant appartenant à votre société et qui est utilisé pour contrôler l'accès à iDRAC6.<br><br>**REMARQUE :** iDRAC6 accepte uniquement les certificats X509 encodés en base 64. Les certificats encodés DER ne sont pas acceptés. Téléversez un nouveau certificat pour remplacer le certificat par défaut que vous avez reçu avec votre iDRAC6. |
| **Afficher le certificat de serveur** | Cette option vous permet d'afficher un certificat de serveur existant. |

## Génération d'une requête de signature de certificat

**REMARQUE :** Chaque nouvelle RSC remplace les données de RSC précédentes stockées sur le micrologiciel. Avant qu'iDRAC ne puisse accepter votre RSC signée, la RSC figurant dans le micrologiciel doit correspondre au certificat renvoyé par l'AC.

1. À la page **SSL**, sélectionnez **Générer une requête de signature de certificat (RSC)**, puis cliquez sur **Suivant**.
2. Sur la page **Générer une requête de signature de certificat (RSC)**, saisissez une valeur pour chaque attribut de la RSC. Le tableau 4-13 décrit les attributs de la RSC.
3. Cliquez sur **Générer** pour créer la RSC et la télécharger sur votre ordinateur local.
4. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 4-14.

**Tableau 4-13. Générer des attributs de requête de signature de certificat (RSC)**

| Champ | Description |
|---|---|
| **Nom commun** | Nom exact à certifier (normalement, le nom de domaine d'iDRAC, par exemple, **www.xyzcompany.com**). Les caractères alphanumériques, les tirets, les traits de soulignement, les espaces et les points sont valides. |
| **Nom de l'organisation** | Nom associé à cette organisation (par exemple, Entreprise XYZ). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides. |
| **Division opérationnelle** | Nom associé à une division opérationnelle, comme un département (par exemple, Informatique). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides. |
| **Ville** | Ville ou autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Seuls les caractères alphanumériques et les espaces sont valides. Ne séparez pas les mots par des traits de soulignement ou d'autres caractères. |
| **Nom de l'état** | État ou province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Seuls les caractères alphanumériques et les espaces sont valides. N'utilisez pas d'abréviations. |
| **Code de pays** | Nom du pays où se trouve l'entité qui fait la demande de certification. |
| **E-mail** | Adresse e-mail associée à la RSC. Tapez l'adresse e-mail de la société ou toute autre adresse e-mail associée à la RSC. Ce champ est optionnel. |

**Tableau 4-14. Boutons de la page Générer une requête de signature de certificat (RSC)**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime les valeurs **Générer une requête de signature de certificat** qui apparaissent à l'écran. |
| **Actualiser** | Recharge la page **Générer une requête de signature de certificat**. |
| **Générer** | Génère une RSC puis invite l'utilisateur à l'enregistrer dans un répertoire spécifié. |
| **Retour au menu principal SSL** | Renvoie l'utilisateur à la page **SSL**. |

## Téléversement d'un certificat de serveur

1. À la page **SSL,** sélectionnez **Téléverser un certificat de serveur**, puis cliquez sur **Suivant**.

   La page **Téléverser un certificat de serveur** s'affiche.

2. Dans le champ **Chemin du fichier**, tapez le chemin du certificat dans le champ **Valeur** ou cliquez sur **Parcourir** pour naviguer vers le fichier du certificat.

**REMARQUE :** La valeur **Chemin du fichier** affiche le chemin de fichier relatif du certificat que vous téléversez. Vous devez saisir le chemin de fichier absolu, qui comprend le chemin et le nom de fichier complets et l'extension du fichier.

3. Cliquez sur **Appliquer**.

4. Cliquez sur le bouton approprié de la page pour continuer. Consultez le tableau 4-15.

**Tableau 4-15. Boutons de la page Téléversement d'un certificat**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime la page **Téléversement d'un certificat**. |
| **Retour au menu principal SSL** | Retourne à la page **Menu principal SSL**. |
| **Appliquer** | Applique le certificat au micrologiciel iDRAC6. |

## Affichage d'un certificat de serveur

1. À la page **SSL,** sélectionnez **Afficher un certificat de serveur**, puis cliquez sur **Suivant**.

   La page **Afficher un certificat de serveur** affiche le certificat de serveur que vous avez téléversé vers iDRAC.

   Le tableau 4-16 décrit les champs et les descriptions associées énumérés dans le tableau **Certificat**.

2. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 4-17.

**Tableau 4-16. Informations relatives au certificat**

| | |
|---|---|

| 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 4-17. Boutons de la page Afficher le certificat de serveur**

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

---

## Configuration et gestion d'Active Directory

La page vous permet de configurer et de gérer les paramètres d'Active Directory.

**REMARQUE :** Vous devez avoir le droit **Configurer iDRAC** afin d'utiliser ou de configurer Active Directory.

**REMARQUE :** Avant de configurer ou d'utiliser la fonctionnalité Active Directory, assurez-vous que votre serveur Active Directory est configuré pour communiquer avec iDRAC6.

**REMARQUE :** Pour de plus amples informations sur la configuration d'Active Directory et la manière de configurer Active Directory avec le schéma détaillé ou le schéma standard, consultez « Utilisation du service de répertoire iDRAC6 ».

Pour accéder à la page **Configuration et gestion d'Active Directory :**

1. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**.
2. Cliquez sur **Active Directory** pour ouvrir la page **Configuration et gestion d'Active Directory**.

   Le tableau 4-18 énumère les options de la page **Configuration et gestion d'Active Directory**.
3. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 4-19.

**Tableau 4-18. Options de la page Configuration et gestion d'Active Directory**

| Attribut | Description |
|---|---|
| **Paramètres communs** | |
| **Active Directory activé** | Spécifie si Active Directory est activé ou désactivé. |
| **Connexion directe activée** | Spécifie si la connexion directe est activée ou désactivée. Si elle est activée, vous pouvez ouvrir une session sur iDRAC6 sans saisir vos références d'utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Les valeurs sont **Oui** et **Non**. |
| **Sélection de schéma** | Spécifie si le schéma standard ou le schéma étendu est utilisé avec Active Directory.<br><br>**REMARQUE :** Dans cette version, les fonctionnalités Authentification bifactorielle (TFA) et Connexion directe (SSO) basées sur une carte à puce ne sont pas prises en charge si Active Directory est configuré pour le schéma étendu. |
| **Nom de domaine de l'utilisateur** | Cette valeur contient jusqu'à 40 entrées de domaine d'utilisateur. Si elle est configurée, la liste des noms de domaine d'utilisateur apparaît dans la page d'ouverture de session comme un menu déroulant à partir duquel l'utilisateur d'ouverture de session doit effectuer un choix. Si elle n'est pas configurée, les utilisateurs d'Active Directory sont toujours en mesure d'ouvrir une session en saisissant le nom d'utilisateur au format nom_d'utilisateur@nom_de_domaine, nom_de_domaine/nom_d'utilisateur ou nom_de-_domaine\nom_d'utilisateur. |
| **Délai d'expiration** | Spécifie la durée, en secondes, accordée aux requêtes Active Directory pour qu'elles se terminent. La valeur par défaut est 120 secondes. |
| **Adresse du serveur du contrôleur de domaine 1-3 (FQDN ou IP)** | Spécifie le nom de domaine pleinement qualifié (FQDN) du contrôleur de domaine ou de l'adresse IP. Au moins une des 3 adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si le schéma étendu est sélectionné, il s'agira des adresses des contrôleurs de domaine dans lesquels l'objet Périphérique 'iDRAC6 et les objets Association sont situés. Si le schéma standard est sélectionné, il s'agit des adresses des contrôleurs de domaine dans lesquels les comptes d'utilisateur et les groupes de rôles sont situés. |
| **Validation de certificat activée** | iDRAC6 utilise le protocole SSL (Security Socket Layer) lors de la connexion à Active Directory. Par défaut, iDRAC6 utilise le certificat d'une AC chargé dans iDRAC6 pour valider le certificat de serveur SSL (Security Socket Layer) des contrôleurs de domaine durant l'établissement de liaisons SSL (Security Socket Layer) et fournit une sécurité accrue. La validation du certificat peut être désactivée à des fins de test ou bien l'administrateur système choisit de se fier aux contrôleurs de domaine dans la limite de sécurité sans valider leurs certificats SSL (Security Socket Layer). Cette option spécifie si la validation du certificat est activée ou désactivée. |

| Certificat d'AC Active Directory | |
|---|---|
| **Certificat** | Certificat de l'autorité de certificat qui signe les certificats de serveur SSL (Security Socket Layer) de tous les contrôleurs de domaine. |
| **Paramètres du schéma étendu** | **Nom iDRAC :** spécifie le nom qui identifie de manière unique iDRAC dans Active Directory. Cette valeur est NULL par défaut.<br><br>**Nom de domaine iDRAC :** nom du DNS (chaîne) du domaine où se trouve l'objet iDRAC d'Active Directory. Cette valeur est NULL par défaut.<br><br>Ces paramètres s'affichent uniquement si iDRAC a été configuré en vue d'une utilisation avec un schéma Active Directory étendu. |
| **Paramètres du schéma standard** | **Adresse du serveur de catalogue global 1-3 (FQDN ou IP) :** spécifie le nom de domaine pleinement qualifié (FQDN) ou l'adresse IP du ou des serveurs de catalogue global. Au moins une des 3 adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Le serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.<br><br>**Groupes de rôles :** spécifie la liste des groupes de rôles associés à iDRAC6.<br><br>**Nom du groupe :** spécifie le nom qui identifie le groupe de rôles dans Active Directory associé à iDRAC6.<br><br>**Domaine du groupe :** spécifie le domaine du groupe.<br><br>**Privilège du groupe :** spécifie le niveau de privilège du groupe.<br><br>Ces paramètres s'affichent uniquement si iDRAC a été configuré en vue d'une utilisation avec un schéma Active Directory standard. |

**Tableau 4-19. Boutons de la page Configuration et gestion d'Active Directory**

| Bouton | Définition |
|---|---|
| **Imprimer** | Imprime les valeurs qui sont affichées à la page Configuration et gestion d'Active Directory. |
| **Actualiser** | Rafraîchit la page Configuration et gestion d'Active Directory. |
| **Configurer Active Directory** | Vous permet de configurer Active Directory. Consultez « Utilisation du service de répertoire iDRAC6 » pour obtenir des informations détaillées sur la configuration. |
| **Paramètres du test** | Vous permet de tester la configuration d'Active Directory à l'aide des paramètres que vous avez spécifiés. Consultez « Utilisation du service de répertoire iDRAC6 » pour obtenir des informations détaillées sur l'utilisation de l'option **Paramètres de test**. |

## Configuration et gestion de LDAP générique

iDRAC6 fournit une solution générique visant à prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne nécessite pas d'extension de schéma sur vos services de répertoire. Pour des informations relatives à la configuration du service de répertoire LDAP générique, consultez « Service de répertoire LDAP générique ».

## Configuration des services iDRAC6

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

1. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**. Cliquez sur l'onglet **Services** pour afficher la page de configuration **Services**.
2. Configurez les services suivants, si nécessaire :
   - Configuration locale : consultez le tableau 4-20
   - Serveur Web : consultez le tableau 4-21 pour les paramètres du serveur Web
   - SSH : consultez le tableau 4-22 pour les paramètres SSH
   - Telnet : consultez le tableau 4-23 pour les paramètres Telnet
   - RACADM distante : consultez le tableau 4-24 pour les paramètres de la RACADM distante
   - Agent SNMP : consultez le tableau 4-25 pour les paramètres SNMP
   - Agent de récupération de système automatique (ASR) : consultez le tableau 4-26 pour les paramètres Agent ASR.
3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 4-27.

**Tableau 4-20. Configuration locale**

| Paramètre | Description |
|---|---|
| **Désactiver la configuration locale d'iDRAC à l'aide de l'option ROM** | Désactive la configuration locale d'iDRAC à l'aide de l'option ROM. L'option ROM se trouve dans le BIOS et fournit un moteur d'interface utilisateur qui permet la configuration de BMC et d'iDRAC. L'option ROM vous invite à saisir le module de configuration en appuyant sur <Ctrl+E>. |
| **Désactiver la configuration locale d'iDRAC avec la RACADM** | Désactive la configuration locale d'iDRAC à l'aide de la RACADM locale. |

**Tableau 4-21. Paramètres du serveur Web**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive le serveur Web iDRAC6. Lorsqu'elle est cochée, cette case indique que le serveur Web est activé. **Activé** est sélectionné par défaut. |
| **Nombre maximal de sessions** | Nombre maximal de sessions simultanées du serveur Web autorisées pour ce système. Ce champ ne peut pas être modifié. Le nombre maximal de sessions simultanées est cinq. |
| **Sessions actives** | Nombre de sessions actuelles sur le système, inférieur ou égal à la value **Nombre maximal de sessions**. Ce champ ne peut pas être modifié. |
| **Délai d'expiration** | Durée, en secondes, pendant laquelle une connexion peut rester inactive. La session est annulée quand le délai d'expiration est atteint. Les modifications apportées aux paramètres Délai d'expiration prennent immédiatement effet et mettent fin à la session d'interface Web en cours. Le serveur Web est également réinitialisé. Veuillez attendre quelques minutes avant d'ouvrir une nouvelle session d'interface Web. La plage du délai d'expiration est de 60 à 10 800 secondes. La valeur par défaut est de 1 800 secondes. |
| **Numéro de port HTTP** | Port sur lequel iDRAC6 écoute une connexion au navigateur. Le numéro de port par défaut est **80**. |
| **Numéro de port HTTPS** | Port sur lequel iDRAC6 écoute une connexion au navigateur sécurisée. Le numéro de port par défaut est **443**. |

**Tableau 4-22. Paramètres SSH**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive SSH. Lorsqu'il est coché, SSH est activé. |
| **Nombre maximal de sessions** | Nombre maximal de sessions SSH simultanées autorisées pour ce système. Vous ne pouvez pas modifier ce champ.<br><br>**REMARQUE :** iDRAC6 prend en charge jusqu'à 2 sessions SSH simultanées. |
| **Sessions actives** | Nombre de sessions SSH actuelles sur le système, inférieur ou égal au paramètre **Nombre maximal de sessions**. Vous ne pouvez pas modifier ce champ. |
| **Délai d'expiration** | Délai d'expiration en cas d'inactivité Secure Shell, en secondes. La plage du délai d'expiration est de 60 à 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. Le numéro de port par défaut est **22**. |

**Tableau 4-23. Paramètres Telnet**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé. |
| **Nombre maximal de sessions** | Nombre maximal de sessions Telnet simultanées autorisées pour ce système. Vous ne pouvez pas modifier ce champ.<br><br>**REMARQUE :** iDRAC6 prend en charge jusqu'à 2 sessions Telnet simultanément. |
| **Sessions actives** | Nombre de sessions Telnet actuelles sur le système, inférieur ou égal au paramètre **Nombre maximal de sessions**. Vous ne pouvez pas modifier ce champ. |
| **Délai d'expiration** | Délai d'expiration en cas d'inactivité 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. Le numéro de port par défaut est **23**. |

**Tableau 4-24. Paramètres de la RACADM distante**

| Paramètre | Description |
|---|---|
| **Activé** | Active/Désactive la RACADM distante. Lorsqu'il est coché, la RACADM distante est activée. |
| **Sessions actives** | Nombre de sessions de la RACADM distante actuelles sur le système. Vous ne pouvez pas modifier ce champ. |

**Tableau 4-25. Paramètres SNMP**

| Paramètre | Description |
|---|---|
| **Activé** | Active/Désactive SNMP. Lorsqu'il est coché, SNMP est activé. |
| **Nom de la communauté SNMP** | Active/Désactive le nom de la communauté SNMP. Lorsqu'il est coché, le nom de la communauté SNMP est activé. Nom de la communauté qui contient l'adresse IP pour la destination des alertes SNMP. Le nom de la communauté peut contenir jusqu'à 31 caractères non blancs. La valeur par défaut est **public**. |

**Tableau 4-26. Paramètre Agent de récupération de système automatique**

| Paramètre | Description |
|---|---|
| **Activé** | Active/Désactive l'agent de récupération de système automatique. Lorsqu'il est coché, l'agent de récupération de système automatique est activé. |

**Tableau 4-27. Boutons de la page Services**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime la page **Services**. |
| **Actualiser** | Actualise la page **Services**. |
| **Appliquer** | Applique les paramètres de la page **Services**. |

---

# Mise à jour de l'image de récupération des services du micrologiciel iDRAC6/système

**REMARQUE :** Si le micrologiciel iDRAC6 devient corrompu, ce qui peut être le cas lorsque la progression de la mise à jour du micrologiciel iDRAC6 est interrompue avant qu'elle ne se termine, vous pouvez récupérer iDRAC6 à l'aide de l'interface Web iDRAC6.

**REMARQUE :** Par défaut, la mise à jour du micrologiciel conserve les paramètres iDRAC6 actuels. Lors du processus de mise à jour, vous avez la possibilité de réinitialiser les paramètres d'usine de la configuration d'iDRAC6. Si vous définissez la configuration sur les paramètres d'usine, vous devez configurer le réseau à l'aide de l'utilitaire de configuration d'iDRAC6.

1. Ouvrez l'interface Web d'iDRAC6 et ouvrez une session sur le système distant.
2. Cliquez sur **Accès à distance**, puis cliquez sur l'onglet **Mettre à jour**.
3. Sur la page **Téléverser/Restaurer (Étape 1 sur 3)**, cliquez sur **Parcourir** ou tapez le chemin de l'image de micrologiciel téléchargée à l'adresse **support.dell.com** ou l'image de récupération des services du système.

   **REMARQUE :** Si vous exécutez Firefox, le curseur de texte n'apparaît pas dans le champ **Image de micrologiciel**.

   Par exemple :

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

   OU

   `\\192.168.1.10\Mises à jour\V1.0\<nom_de_l'image>`

   Par défaut, le nom de l'image de micrologiciel est **firmimg.d6**.
4. Cliquez sur **Téléverser**.

   Le fichier va se téléverser vers iDRAC6. Ce processus peut prendre plusieurs minutes.

   Le message suivant s'affiche jusqu'à la fin du processus :

   `File upload in progress... (Téléversement du fichier en cours...)`
5. À la page **Condition (page 2 sur 3)**, vous voyez les résultats de la validation effectuée sur le fichier image que vous avez téléversé.
   - Si le fichier image s'est téléversé avec succès et a passé tous les points de vérification, le nom du fichier image s'affiche. Si l'image de micrologiciel a été téléversée, les versions actuelles et nouvelles du micrologiciel s'affichent.

     OU
   - Si l'image ne s'est pas téléversée avec succès ou si elle n'a pas passé les points de vérification, un message d'erreur approprié s'affiche et la mise à jour retourne à la page **Téléverser/Restaurer (Étape 1 sur 3)**. Vous pouvez réessayer de mettre à jour iDRAC6 ou cliquer sur **Annuler** pour réinitialiser iDRAC6 sur le mode de fonctionnement normal.
6. Dans le cas d'une image de micrologiciel, la fonction **Conserver la configuration** vous donne la possibilité de conserver ou de supprimer la configuration

existante d'iDRAC6. Cette option est sélectionnée par défaut.

**REMARQUE :** Si vous désélectionnez la case à cocher **Conserver la configuration**, les paramètres par défaut d'iDRAC6 sont réinitialisés. Dans les paramètres par défaut, le LAN est activé. Vous ne pouvez pas ouvrir une session sur l'interface Web iDRAC6. Vous devrez reconfigurer les paramètres LAN à l'aide de l'utilitaire de configuration d'iDRAC6 durant le POST du BIOS.

7. Cliquez sur **Mettre à jour** pour démarrer le processus de mise à jour.

8. La page **Mise à jour (Étape 3 sur 3)** affiche la condition de la mise à jour. La progression de la mise à jour, indiquée en pourcentage, apparaît dans la colonne **Progression**.

**REMARQUE :** Lorsque vous êtes en mode mise à jour, le processus de mise à jour continue en fond d'écran même si vous naviguez en dehors de cette page.

Si la mise à jour du micrologiciel est terminée, iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC6 avec une nouvelle fenêtre de navigateur. Un message d'erreur approprié s'affiche si une erreur se produit.

Si la mise à jour de la récupération des services du système réussit/échoue, un message de condition approprié s'affiche.

## Restauration du micrologiciel iDRAC6

iDRAC6 peut maintenir deux images de micrologiciel simultanées. Vous pouvez décider de démarrer à partir de (restaurer vers) l'image de micrologiciel de votre choix.

1. Ouvrez l'interface Web iDRAC6 et ouvrez une session sur le système distant.

   Cliquez sur **Système→ Accès à distance**, puis sur l'onglet **Mettre à jour**.

2. À la page **Téléverser/Restaurer (Étape 1 sur 3)**, cliquez sur **Restaurer**. La version actuelle et la version restaurée du micrologiciel s'affichent à la page **Condition (Étape 2 sur 3)**.

   **Conserver la configuration** vous donne la possibilité de conserver ou de supprimer la configuration iDRAC6 existante. Cette option est sélectionnée par défaut.

   **REMARQUE :** Si vous désélectionnez la case à cocher **Conserver la configuration**, les paramètres par défaut d'iDRAC6 sont réinitialisés. Dans les paramètres par défaut, le LAN est activé. Vous ne pouvez pas ouvrir une session sur l'interface Web iDRAC6. Vous devrez reconfigurer les paramètres LAN à l'aide de l'utilitaire de configuration d'iDRAC6 durant le POST du BIOS ou à l'aide de la commande racadm (disponible localement sur le serveur).

3. Cliquez sur **Mettre à jour** pour démarrer le processus de mise à jour du micrologiciel.

   À la page **Mise à jour (Étape 3 sur 3)**, vous voyez la condition de l'opération de restauration. La progression, indiquée en pourcentage, apparaît dans la colonne **Progression**.

   **REMARQUE :** Lorsque vous êtes en mode mise à jour, le processus de mise à jour continue en fond d'écran même si vous naviguez en dehors de cette page.

   Si la mise à jour du micrologiciel est terminée, iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC6 avec une nouvelle fenêtre de navigateur. Un message d'erreur approprié s'affiche si une erreur se produit.

---

# Syslog distant

La fonctionnalité Syslog distant d'iDRAC6 vous permet d'écrire à distance le journal du RAC et le journal des événements système (SEL) sur un serveur syslog externe. Vous pouvez lire tous les journaux de l'ensemble de la batterie de serveurs à partir d'un journal central.

Le protocole syslog distant ne nécessite aucune authentification de l'utilisateur. Quant aux journaux à saisir dans le serveur syslog distant, assurez-vous de la connectivité réseau entre iDRAC6 et le serveur syslog distant et que le serveur syslog distant s'exécute sur le même réseau qu'iDRAC6. Les entrées du syslog distant sont des paquets UDP (User Datagram Protocol) envoyés au port syslog du serveur syslog distant. En cas de panne réseau, iDRAC6 n'envoie pas le même journal une seconde fois. La journalisation à distance est effectuée en temps réel à mesure que les journaux sont enregistrés dans le journal du RAC et le journal SEL d'iDRAC6.

Le syslog distant peut être activé 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.

3. Dans l'arborescence du système, sélectionnez **Système→** onglet **Configuration→ Paramètres du syslog distant**. L'écran **Paramètres du syslog distant** s'affiche.

Le tableau 4-28 répertorie les paramètres Syslog distant.

**Tableau 4-28. Paramètres Syslog distant**

---

| Attribut | Description |
|---|---|
| Syslog distant activé | Sélectionnez cette option pour activer la transmission et la saisie à distance du syslog sur le serveur spécifié. Lorsque le syslog est activé, de nouvelles entrées de journal sont envoyées à un ou à des serveurs syslog. |
| Serveur syslog 1-3 | Saisissez l'adresse du serveur syslog distant afin de journaliser les messages iDRAC6 tels que le journal SEL et le journal du RAC. Les adresses du serveur syslog peuvent contenir des caractères alphanumériques, -, ., : et _. |
| Numéro de port | Saisissez le numéro de port du serveur syslog distant. Le numéro de port doit être compris entre 1 et 65 535. Le port par défaut est 514. |

**REMARQUE :** Les niveaux de gravité définis par le protocole syslog distant diffèrent des niveaux de gravité standard du journal des événements système (SEL) IPMI. Toutes les entrées du syslog distant iDRAC6 sont ainsi rapportées dans le serveur syslog avec **Avis** comme niveau de gravité.

L'exemple suivant illustre l'utilisation des objets de configuration et de la commande RACADM afin de modifier les paramètres du syslog distant :

```
racadm config –g cfgRemoteHosts –o cfgRhostsSyslogEnable [1/0] ; la valeur par défaut est 0

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogServer1 <nom du serveur 1> ; la valeur par défaut est vide

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogServer2 <nom du serveur 2> ; la valeur par défaut est vide

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogServer3 <nom du serveur 3> ; la valeur par défaut est vide

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogPort <numéro de port> ; la valeur par défaut est 514
```

---

## Périphérique de démarrage initial

Cette fonctionnalité vous permet de sélectionner le périphérique de démarrage initial de votre système et d'activer **Démarrage unique**. Le système démarre à partir du périphérique sélectionné lors des redémarrages suivants et consécutifs, et demeure le périphérique de démarrage initial dans l'ordre de démarrage du BIOS jusqu'à ce qu'il soit remodifié depuis l'IUG iDRAC6 ou depuis la séquence de démarrage du BIOS.

Le périphérique de démarrage initial peut être sélectionné 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.
3. Dans l'arborescence du système, sélectionnez **Système→** onglet **Configuration→ Périphérique de démarrage initial**. L'écran **Périphérique de démarrage initial** s'affiche.

Le tableau 4-29 répertorie les paramètres **Périphérique de démarrage initial**.

**Tableau 4-29. Périphérique de démarrage initial**

| Attribut | Description |
|---|---|
| Périphérique de démarrage initial | Sélectionnez le périphérique de démarrage initial dans la liste déroulante. Le système démarrera à partir du périphérique sélectionné lors des redémarrages suivants et consécutifs. |
| Démarrage unique | Sélectionné = Activé ; désélectionné = Désactivé. Cochez cette option pour effectuer un démarrage à partir du périphérique sélectionné lors du prochain démarrage. Ensuite, le système démarrera à partir du périphérique de démarrage initial dans l'ordre de démarrage du BIOS. |

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration avancée d'iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Contenant des informations sur la configuration avancée d'iDRAC6, cette section est recommandée aux utilisateurs ayant des connaissances avancées en gestion des systèmes et désirant personnaliser l'environnement d'iDRAC6 en fonction de leurs besoins spécifiques.

---

## Avant de commencer

Vous devez avoir terminé l'installation et la configuration de base du matériel et du logiciel de votre iDRAC6. Pour plus d'informations, consultez « Installation de base d'iDRAC6 ».

---

## Configuration d'iDRAC6 pour l'affichage de la sortie série à distance sur SSH/Telnet

Vous pouvez configurer iDRAC6 pour la redirection de console série à distance en procédant de la manière suivante :

Configurez d'abord le BIOS pour activer la redirection de console série :

1. Allumez ou redémarrez votre système.
2. Appuyez sur <F2> dès que vous avez vu le message suivant :

   ```
   <F2> = System Setup (<F2> = configuration système)
   ```

3. Faites défiler la fenêtre et sélectionnez **Serial Communication (Communications série)** en appuyant sur <Entrée>.
4. Définissez les options de l'écran **Serial Communication** comme suit :

   ```
   serial communication....On with serial redirection via com2

   (communications série....Activé avec la redirection série via com2)
   ```

   **REMARQUE :** Vous pouvez définir les communications série sur **On with serial redirection via com1 (Activé avec la redirection série via com1)** tant que le champ Adresse du port série, périphérique série2, est également défini sur com1.

   ```
   serial port address....Serial device1 = com1, serial device2 = com2

   external serial connector....Serial device 1

   failsafe baud rate....115200

   remote terminal type....vt100/vt220

   redirection after boot....Enabled

   (adresse du port série....Périphérique série1 = com1, périphérique série2 = com2

   connecteur série externe....Périphérique série 1

   débit en bauds de secours....115 200

   type de terminal distant....vt100/vt220

   redirection après démarrage....Activé)
   ```

   Sélectionnez ensuite **Save Changes (Enregistrer les modifications)**.

5. Appuyez sur <Échap> pour quitter le programme **Configuration système** et terminer la configuration du programme Configuration système.

## Configuration des paramètres d'iDRAC6 pour activer SSH/Telnet

Configurez ensuite les paramètres iDRAC6 pour activer ssh/Telnet via la RACADM ou l'interface Web iDRAC6.

Pour configurer les paramètres iDRAC6 afin d'activer ssh/Telnet avec la RACADM, exécutez les commandes suivantes :

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

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

Vous pouvez également exécuter les commandes RACADM à distance ; consultez « Utilisation de la RACADM à distance ».

Pour configurer les paramètres iDRAC6 afin d'activer ssh/Telnet à l'aide de l'interface Web iDRAC6, procédez comme suit :

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Services**.
3. Sélectionnez **Activé** dans la section **SSH** ou **Telnet**.
4. Cliquez sur **Appliquer les modifications**.

Connectez-vous ensuite à iDRAC6 via Telnet ou SSH.

## Démarrage d'une console texte via Telnet ou SSH

Lorsque vous avez ouvert une session sur iDRAC6 via le logiciel du terminal de votre station de gestion avec Telnet ou SSH, vous pouvez rediriger la console texte du système géré en utilisant **console com2** qui est une commande Telnet/SSH. Un seul client **console com2** est pris en charge à la fois.

Pour vous connecter à la console texte du système géré, ouvrez une invite de commande iDRAC6 (affichée via une session Telnet ou SSH) et tapez :

```
console com2
```

La commande `console -h com2` affiche le contenu du tampon de l'historique série avant qu'une entrée ne soit faite à partir du clavier ou que de nouveaux caractères ne proviennent du port série.

La taille par défaut (et maximale) du tampon de l'historique est 8 192 caractères. Vous pouvez définir ce nombre sur une valeur plus petite avec la commande :

```
racadm config -g cfgSerial -o cfgSerialHistorySize <nombre>
```

Pour configurer Linux pour la direction de la console pendant le démarrage, consultez « Configuration de Linux pour la redirection de console série pendant le démarrage ».

## Utilisation d'une console Telnet

### Exécution de Telnet avec Microsoft® Windows® XP ou Windows 2003

Si votre station de gestion exécute Windows XP ou Windows 2003, un problème peut surgir au niveau des caractères lors d'une session Telnet iDRAC6. Ce problème peut prendre la forme d'une ouverture de session figée, la touche Retour ne répondant pas et l'invite de mot de passe n'apparaissant pas.

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

### Exécution de Telnet à l'aide de Windows 2000

Si votre station de gestion exécute Windows 2000, vous ne pouvez pas accéder à la configuration du BIOS en appuyant sur la touche <F2>. Pour résoudre ce problème, utilisez le client Telnet fourni avec le téléchargement gratuit recommandé de Windows Services for UNIX® 3.5 de Microsoft. Accédez à **www.microsoft.com/downloads/** et recherchez « *Windows Services for UNIX 3.5* ».

### Activation de Microsoft Telnet pour la redirection de console Telnet

**REMARQUE :** Certains clients Telnet fonctionnant sous les systèmes d'exploitation Microsoft risquent de ne pas pouvoir afficher correctement l'écran de configuration du BIOS lorsque la redirection de console du BIOS est définie pour l'émulation VT100/VT220. Si ce problème se produit, mettez à jour l'affichage en choisissant le mode ANSI pour la redirection de console du BIOS. Pour effectuer cette procédure dans le menu de configuration du BIOS, sélectionnez **Redirection de console** → **Type de terminal distant** → **ANSI**.

**REMARQUE :** Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console redirigée sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement ; sinon, certains écrans de texte risquent d'être illisibles.

1. Activez **Telnet** dans **Services du composant Windows.**

2. Connectez-vous à iDRAC6 sur la station de gestion.

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

   `telnet <adresse IP>:<numéro de port>`

   où *adresse IP* est l'adresse IP d'iDRAC6 et *numéro de port* est le numéro de port Telnet (si vous utilisez un nouveau port).

### Configuration de la touche Retour arrière pour votre session Telnet

Selon le client Telnet, l'utilisation de la touche <Retour> 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 Microsoft Telnet pour qu'ils utilisent la touche <Retour> :

1. Ouvrez une fenêtre d'invite de commande (si nécessaire).

2. Si vous n'exécutez pas déjà de session Telnet, tapez :

   `telnet`

   Si vous exécutez une session Telnet, appuyez sur <Ctrl><]>.

3. À l'invite, tapez :

   `set bsasdel`

   Le message suivant s'affiche :

   `Backspace will be sent as delete. (Retour arrière sera envoyé en tant que supprimer.)`

Pour configurer une session Linux Telnet pour qu'elle utilise la touche <Retour> :

1. Ouvrez une invite de commande et tapez :

   `stty erase ^h`

2. À l'invite, tapez :

   `telnet`

## Utilisation de Secure Shell (SSH)

Il est essentiel que les périphériques de votre système et la gestion des périphériques soient sécurisés. Les périphériques connectés intégrés sont au cur de nombreux processus d'affaires. Si ces périphériques sont compromis, votre entreprise peut être menacée, ce qui exige de nouvelles demandes de sécurité pour le logiciel de gestion de périphériques de l'interface de ligne de commande (CLI).

Secure Shell (SSH) est une session de ligne de commande qui inclut les mêmes capacités qu'une session Telnet, mais avec une sécurité accrue. iDRAC6 prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé sur iDRAC6 lorsque vous installez ou mettez à jour votre micrologiciel iDRAC6.

Vous pouvez utiliser PuTTY ou OpenSSH sur la station de gestion pour vous connecter à l'iDRAC6 du système géré. Lorsqu'une erreur se produit pendant la procédure d'ouverture de session, le client secure shell émet 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 l'invite de commande Windows n'offre pas une fonctionnalité complète (quelques touches ne répondent pas et aucun graphique n'est affiché).

Seules quatre sessions SSH sont prises en charge à la fois. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout` comme décrit dans « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

Pour activer SSH sur iDRAC6, tapez :

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

Pour changer le port SSH, tapez :

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <numéro de port>
```

Pour plus d'informations sur les propriétés `cfgSerialSshEnable` et `cfgRacTuneSshPort`, consultez « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

L'implémentation SSH iDRAC6 prend en charge plusieurs schémas de cryptographie, comme illustré dans le tableau 5-1.

**Tableau 5-1. Schémas de cryptographie**

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

**REMARQUE :** SSHv1 n'est pas pris en charge.

## Configuration de Linux pour la redirection de console série pendant le démarrage

Les étapes suivantes sont spécifiques au chargeur GRUB (GRand Unified Bootloader) de Linux. Des modifications similaires devront être apportées si vous utilisez un chargeur de démarrage différent.

**REMARQUE :** Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console redirigée sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement ; sinon, certains écrans de texte risquent d'être illisibles.

Modifiez le fichier **/etc/grub.conf** de la manière suivante :

1. Localisez les sections Paramètres généraux dans le fichier et ajoutez les deux nouvelles lignes suivantes :

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

2. Ajoutez deux options à la ligne du noyau :

   ```
   kernel console=ttyS1,115200n8r console=tty1
   ```

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

Le tableau 5-2 fournit un exemple de fichier **/etc/grub.conf** qui illustre les modifications décrites dans cette procédure.

**Tableau 5-2. Exemple de fichier : /etc/grub.conf**

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Lorsque vous modifiez le fichier **/etc/grub.conf**, observez les instructions suivantes :

1. Désactivez l'interface graphique du GRUB et utilisez l'interface texte ; sinon, l'écran du GRUB ne s'affichera pas sur la redirection de console du RAC. Pour désactiver l'interface graphique, commentez la ligne commençant par `splashimage`.

2. Pour activer plusieurs options GRUB afin de démarrer les sessions de console via la connexion série du RAC, ajoutez la ligne suivante à toutes les options :

   ```
   console=ttyS1,115200n8r console=tty1
   ```

   Le tableau 5-2 illustre l'ajout de `console=ttyS1,57600` uniquement à la première option.

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

Modifiez le fichier **/etc/inittab** comme suit :

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

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

Le tableau 5-3 illustre un exemple de fichier avec la nouvelle ligne.

**Tableau 5-3. Exemple de fichier : /etc/innitab**

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifiez le fichier **/etc/securetty** comme suit :

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

```
ttyS1
```

Le tableau 5-4 illustre un exemple de fichier avec la nouvelle ligne.

**Tableau 5-4. Exemple de fichier : /etc/securetty**

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

---

## Configuration d'iDRAC6 pour la connexion série

Vous pouvez utiliser l'une des interfaces suivantes pour vous connecter à iDRAC6 via la connexion série :

- CLI iDRAC6
- Connexion directe en mode de base
- Connexion directe en mode terminal

Pour configurer votre système en vue de l'utilisation de ces interfaces, procédez de la manière suivante :

Configurez le **BIOS** pour activer la connexion série :

1. Allumez ou redémarrez votre système.
2. Appuyez sur <F2> dès que vous avez vu le message suivant :

   ```
   <F2> = System Setup (<F2> = configuration système)
   ```

3. Faites défiler la fenêtre et sélectionnez **Serial Communication (Communications série)** en appuyant sur <Entrée>.
4. Définissez l'écran **Serial Communication** comme suit :

   connecteur série externe....périphérique d'accès à distance

   Sélectionnez ensuite **Save Changes (Enregistrer les modifications)**.

5. Appuyez sur <Échap> pour quitter le programme **Configuration système** et terminer la configuration du programme Configuration système.

Connectez ensuite votre câble DB-9 ou null modem de la station de gestion au serveur de nud géré. Consultez « Connexion du câble DB-9 ou null modem pour la console série ».

Assurez-vous ensuite que votre logiciel d'émulation du terminal de gestion est configuré pour la connexion série. Consultez « Configuration du logiciel d'émulation de terminal de la station de gestion ».

Configurez ensuite les paramètres d'iDRAC6 pour activer les connexions série via la RACADM ou l'interface Web iDRAC6.

Pour configurer les paramètres d'iDRAC6 afin d'activer les connexions séries à l'aide de la RACADM, exécutez la commande suivante :

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

Pour configurer les paramètres d'iDRAC6 afin d'activer les connexions séries à l'aide de l'interface Web iDRAC6, procédez de la manière suivante :

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Sélectionnez **Activé** dans la section **Série RAC**.

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

Lorsque vous êtes connecté en série à l'aide des paramètres précédents, une invite d'ouverture de session s'affiche. Saisissez le nom d'utilisateur et le mot de passe iDRAC6 (les valeurs par défaut sont respectivement `root` et `calvin`).

Dans cette interface, vous pouvez exécuter des fonctionnalités telles que la RACADM. Par exemple, pour imprimer le journal des événements système, saisissez la commande RACADM suivante :

```
racadm getsel
```

## Configuration d'iDRAC pour la connexion directe en mode de base et en mode terminal

À l'aide de la RACADM, exécutez la commande suivante pour désactiver l'interface de ligne de commande d'iDRAC6 :

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

Exécutez ensuite la commande RACADM suivante pour activer la connexion directe en mode de base :

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 1
```

Vous pouvez également exécuter la commande RACADM suivante pour activer la connexion directe en mode terminal :

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 0
```

Vous pouvez effectuer les mêmes actions en utilisant l'interface Web iDRAC6 :

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Désélectionnez **Activé** dans la section **Série RAC**.

   Pour la connexion directe en mode de base :

   Dans la section **Série IPMI**, faites passer le menu déroulant **Paramètres du mode de connexion** à **Connexion directe en mode de base**.

   Pour la connexion directe en mode terminal :

   Dans la section **Série IPMI**, faites passer le menu déroulant **Paramètres du mode de connexion** à **Connexion directe en mode terminal**.
4. Cliquez sur **Appliquer les modifications**. Pour plus d'informations sur la connexion directe en mode de base et en mode terminal, consultez « Configuration des modes série et terminal ».

La connexion directe en mode de base vous permet d'utiliser des outils tels qu'ipmish directement via la connexion série. Par exemple, pour imprimer le journal des événements système à l'aide d'ipmish via le mode de base IPMI, exécutez la commande suivante :

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```

La connexion directe en mode terminal vous permet d'émettre des commandes ASCII sur iDRAC6. Par exemple, pour activer/désactiver le serveur via la connexion directe en mode terminal :

1. Connectez-vous à iDRAC6 via le logiciel d'émulation de terminal.
2. Tapez la commande suivante pour ouvrir une session :

   ```
   [SYS PWD -U root calvin]
   ```

   Les éléments suivants s'affichent alors :

   ```
   [SYS]
   ```

   ```
   [OK]
   ```
3. Tapez la commande suivante pour vous assurer que l'ouverture de session a réussi :

   ```
   [SYS TMODE]
   ```

   Les éléments suivants s'affichent alors :

   ```
   [OK TMODE]
   ```
4. Pour désactiver le serveur (le serveur se désactive immédiatement), tapez la commande suivante :

   ```
   [SYS POWER OFF]
   ```

5. Pour activer le serveur (le serveur s'active immédiatement) :

   ```
   [SYS POWER ON]
   ```

## Commutation entre le mode vommunication d'interface série du RAC et Redirection de console série

iDRAC6 prend en charge les séquences de la touche Échap permettant de commuter entre la communication d'interface série du RAC et la redirection de console série.

Pour définir votre système de manière à ce qu'il autorise ce comportement, procédez comme suit :

1. Allumez ou redémarrez votre système.
2. Appuyez sur <F2> dès que vous avez vu le message suivant :

   ```
   <F2> = System Setup (<F2> = configuration système)
   ```

3. Faites défiler la fenêtre et sélectionnez **Serial Communication (Communications série)** en appuyant sur <Entrée>.
4. Définissez l'écran **Serial Communication** comme suit :

   serial communication -- On with serial redirection via com2

   **REMARQUE :** Vous pouvez définir le champ **serial communication (Communications série)** sur **On with serial redirection via com1 (Activé avec la redirection série via com1)** si le **serial device2 (périphérique série2)** du champ **serial port address (Adresse du port série)** est également défini sur com1.

   serial port address -- Serial device1 = com1, serial device2 = com2

   external serial connector -- Serial device 2

   failsafe baud rate....115200

   remote terminal type ...vt100/vt220

   redirection after boot ... Enabled

   Sélectionnez ensuite **Enregistrer les modifications**.

5. Appuyez sur <Échap> pour quitter le programme **Configuration système** et terminer la configuration du programme Configuration système.

Connectez le câble null modem entre le connecteur série externe du système géré et le port série de la station de gestion.

Utilisez un programme d'émulation de terminal (HyperTerminal ou TeraTerm) sur la station de gestion et, en fonction de l'avancement du processus de démarrage du serveur géré, les écrans du POST ou les écrans du système d'exploitation apparaissent. Ceci repose sur la configuration : SAC pour Windows et les écrans en mode texte Linux pour Linux. Définissez les paramètres de terminal de la station de gestion : Débit en bauds :115 200 ; données : 8 bits ; parité : aucune ; arrêt : 1 bit et contrôle du débit : aucun.

Pour passer au mode communication d'interface série du RAC lorsque vous vous trouvez en mode redirection de console série, utilisez la séquence de touches suivante :

```
<Échap> + <Maj> <9>
```

La séquence de touches ci-dessus vous dirige vers l'invite « Ouverture de session sur iDRAC » (si le RAC est défini sur le mode « RAC série ») ou le mode « Connexion série » où les commandes de terminal peuvent être émises (si le RAC est défini sur « Connexion directe IPMI série en mode terminal »).

Pour passer au mode redirection de console série lorsque vous êtes en mode communication d'interface série du RAC, utilisez la séquence de touches suivante :

```
<Échap> + <Maj> <q>
```

---

# Connexion du câble DB-9 ou null modem pour la console série

Pour accéder au système géré en utilisant une console texte série, connectez un DB-9 ou null modem au port COM du système géré. Pour que la connexion fonctionne avec le câble null modem, les paramètres de communications série correspondants doivent être définis dans la configuration CMOS. Certains des câbles DB-9 n'ont pas le brochage/les signaux requis pour cette connexion. Le câble DB-9 utilisé pour cette connexion doit avoir les spécifications décrites dans le tableau 5-5.

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

**Tableau 5-5. Brochage requis pour le câble DB-9 ou null modem**

| | | |
|---|---|---|

| Nom du signal | Broche DB-9 (broche du serveur) | Broche DB-9 (broche de la station de travail) |
|---|---|---|
| FG (masse de l'armature) | - | - |
| TD (transmission de données) | 3 | 2 |
| RD (réception de données) | 2 | 3 |
| RTS (demande d'envoi) | 7 | 8 |
| CTS (prêt à envoyer) | 8 | 7 |
| SG (terre du signal) | 5 | 5 |
| DSR (ensemble de données prêt) | 6 | 4 |
| CD (détection de porteuse) | 1 | 4 |
| DTR (terminal de données prêt) | 4 | 1 et 6 |

---

# Configuration du logiciel d'émulation de terminal de la station de gestion

iDRAC6 prend en charge une console texte série ou Telnet d'une station de gestion exécutant l'un des types de logiciel d'émulation de terminal suivants :

- Linux Minicom dans un Xterm
- HyperTerminal Private Edition (version 6.3) de Hilgraeve
- Linux Telnet dans un Xterm
- Microsoft Telnet

Effectuez les étapes des sous-sections suivantes pour configurer votre type de logiciel de terminal. Si vous utilisez Microsoft Telnet, la configuration n'est pas nécessaire.

## Configuration de Linux Minicom pour l'émulation de console série

Minicom est l'utilitaire d'accès au port série pour Linux. Les étapes suivantes s'appliquent pour configurer Minicom version 2.0. Les autres versions de Minicom peuvent être légèrement différentes, mais elles requièrent les mêmes paramètres de base. Utilisez les informations dans « Paramètres de Minicom requis pour l'émulation de console série » pour configurer d'autres versions de Minicom.

### Configuration de Minicom version 2.0 pour l'émulation de console série

**REMARQUE :** Pour que le texte s'affiche correctement, il est recommandé d'utiliser une fenêtre Xterm plutôt que la console par défaut fournie lors de l'installation de Linux pour afficher la console Telnet.

1. Pour lancer une nouvelle session Xterm, tapez `xterm &` à l'invite de commande.
2. Dans la fenêtre Xterm, déplacez le curseur de la souris dans le coin inférieur droit de la fenêtre et redimensionnez la fenêtre sur 80 x 25.
3. Si vous n'avez pas de fichier de configuration Minicom, passez à l'étape suivante.

   Si vous avez un fichier de configuration Minicom, tapez `minicom <nom du fichier de configuration Minicom>` et passez à étape 17.
4. À l'invite de commande Xterm, tapez `minicom -s`.
5. Sélectionnez **Configuration du port série** et appuyez sur <Entrée>.
6. Appuyez sur <a> et sélectionnez le périphérique série approprié (**/dev/ttySo**, par exemple).
7. Appuyez sur <e> et définissez l'option **Bis/Par/Bits** sur **57600 8N1**.
8. Appuyez sur <f>, définissez **Contrôle du débit matériel** sur **Oui** et définissez **Contrôle du débit logiciel** sur **Non**.
9. Pour quitter le menu **Configuration du port série**, appuyez sur <Entrée>.
10. Sélectionnez **Modem et numérotation** et appuyez sur <Entrée>.
11. Dans le menu **Configuration de la numérotation du modem et des paramètres**, appuyez sur <Retour> pour effacer les paramètres **init**, **reset**, **connect** et **hangup** et les laisser vides.
12. Pour enregistrer chaque valeur vide, appuyez sur <Entrée>.
13. Lorsque tous les champs indiqués sont effacés, appuyez sur <Entrée> pour quitter le menu **Configuration de la numérotation du modem et des paramètres**.

14. Sélectionnez **Enregistrer la configuration sous config_name** et appuyez sur <Entrée>.

15. Sélectionnez **Quitter Minicom** et appuyez sur <Entrée>.

16. À l'invite de l'environnement de commande, tapez `minicom <nom du fichier de configuration Minicom>`.

17. Pour agrandir la fenêtre de Minicom à 80 x 25, faites glisser le coin de la fenêtre.

18. Appuyez sur <Ctrl+a>, <z>, <x> pour quitter Minicom.

**REMARQUE :** Si vous utilisez Minicom pour la redirection de console texte série afin de configurer le BIOS du système géré, il est recommandé d'activer la couleur dans Minicom. Pour activer la couleur, tapez la commande suivante : `minicom -c on`

Assurez-vous que la fenêtre Minicom affiche une invite de commande. Lorsque l'invite de commande apparaît, votre connexion est réussie et vous pouvez vous connecter à la console du système géré avec la commande série **connect**.

### Paramètres de Minicom requis pour l'émulation de console série

Utilisez le tableau 5-6 pour configurer une version quelconque de Minicom.

**Tableau 5-6. Paramètres de Minicom pour l'émulation de console série**

| Description du paramètre | Paramètre requis |
|---|---|
| B/s/Par/Bits | 57600 8N1 |
| Contrôle du débit matériel | Oui |
| Contrôle du débit logiciel | Non |
| Émulation de terminal | ANSI |
| Paramètres de la numérotation du modem et des paramètres | Effacez les paramètres **init**, **reset**, **connect** et **hangup** pour qu'ils soient vides |
| Taille de fenêtre | 80 x 25 (pour redimensionner, faites glisser le coin de la fenêtre) |

## Configuration d'HyperTerminal pour la redirection de console série

HyperTerminal est l'utilitaire d'accès au port série de Microsoft Windows. Pour définir correctement la taille de l'écran de votre console, utilisez HyperTerminal Private Edition version 6.3 de Hilgraeve.

**PRÉCAUTION : Toutes les versions de système d'exploitation Microsoft Windows comprennent le logiciel d'émulation de terminal HyperTerminal de Hilgraeve. Cependant, la version comprise ne fournit pas beaucoup de fonctions requises pendant la redirection de console. À la place, vous pouvez utiliser tout logiciel d'émulation de terminal qui prend en charge le mode d'émulation VT100/VT220 ou ANSI. Un exemple d'émulateur de terminal complet VT100/VT220 ou ANSI qui prend en charge la redirection de console sur votre système est HyperTerminal Private Edition 6.3 de Hilgraeve. En outre, l'utilisation de la fenêtre de ligne de commande pour effectuer une redirection de console série Telnet risque d'afficher des caractères parasites.**

Pour configurer HyperTerminal pour la redirection de console série :

1. Lancez le programme HyperTerminal.

2. Tapez le nom de la nouvelle connexion et cliquez sur **OK**.

3. À côté de **Connecter en utilisant :**, sélectionnez le port COM de la station de gestion (COM2, par exemple) auquel vous avez connecté le câble DB-9 ou null modem et cliquez sur **OK**.

4. Configurez les paramètres du port COM comme indiqué dans le tableau 5-7.

5. Cliquez sur **OK**.

6. Cliquez sur **Fichier**→ **Propriétés**, puis sur l'onglet **Paramètres**.

7. Définissez la **Référence du terminal Telnet :** sur **ANSI**.

8. Cliquez sur **Configuration du terminal** et choisissez **26** pour **Lignes de l'écran**.

9. Définissez **Colonnes** sur **80** et cliquez sur **OK**.

**Tableau 5-7. Paramètres du port COM de la station de gestion**

| Description du paramètre | Paramètre requis |
|---|---|
| Bits par seconde | 57 600 |
| Bits de données | 8 |
| Parité | Aucun |
| Bits d'arrêt | 1 |
| Contrôle du débit | Matériel |

---

# Configuration des modes série et terminal

## Configuration du mode série IPMI et iDRAC6

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Configurez les paramètres série IPMI.

   Consultez le tableau 5-8 pour une description des paramètres série IPMI.
4. Configurez les paramètres série d'iDRAC6.

   Consultez le tableau 5-9 pour une description des paramètres série d'iDRAC6.
5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur le bouton approprié de la page **Série** pour continuer. Consultez le tableau 5-10 pour obtenir une description des paramètres de la page Configuration série.

**Tableau 5-8. Paramètres série IPMI**

| Paramètre | Description |
|---|---|
| **Paramètres du mode de connexion** | • Connexion directe en mode de base : mode de base série IPMI<br>• Connexion directe en mode terminal : mode terminal série IPMI |
| **Débit en bauds** | • Définit la vitesse de transmission de données. Sélectionnez **9 600 b/s**, **19,2 kb/s**, **57,6 kb/s** ou **115,2 kb/s**. |
| **Contrôle du débit** | • Aucun : contrôle du débit matériel désactivé<br>• RTS/CTS : contrôle du débit matériel activé |
| **Limite du niveau de privilège du canal** | • Administrateur<br>• Opérateur<br>• Utilisateur |

**Tableau 5-9. Paramètres série iDRAC6**

| Paramètre | Description |
|---|---|
| **Activé** | Active ou désactive la console série iDRAC6. Coché = Activé ; décoché = Désactivé |
| **Délai d'expiration** | La durée maximale d'inactivité de la ligne, en secondes, qui doit s'écouler avant que la ligne ne soit déconnectée La plage est comprise entre 60 et 1 920 secondes. La valeur par défaut est 300 secondes. Utilisez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. |
| **Redirection activée** | Active ou désactive la redirection de console. Coché = Activé ; décoché = Désactivé |
| **Débit en bauds** | Vitesse de transmission de données sur le port série externe. Les valeurs sont les suivantes : **9 600 b/s**, **19,2 kb/s**, **57,6 kb/s** et **115,2 kb/s**. La valeur par défaut est **57,6 kb/s**. |
| **Touche Échap** | Spécifie la touche <Échap>. Les caractères ^\ sont définis par défaut. |
| **Taille du tampon de l'historique** | Taille du tampon de l'historique série qui contient les derniers caractères écrits sur la console. La valeur maximale et par défaut est de 8 192 caractères. |
| **Commande d'ouverture de session** | Ligne de commande iDRAC6 à exécuter lors d'une ouverture de session valide. |

**Tableau 5-10. Paramètres de la page Série**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprimer la page **Série**. |
| **Actualiser** | Actualisez la page **Série**. |
| **Appliquer les modifications** | Appliquez les modifications série IPMI et iDRAC6. |
| **Paramètres du mode terminal** | Ouvre la page **Paramètres du mode terminal**. |

## Configuration du mode terminal

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Sur la page **Série**, cliquez sur **Paramètres du mode terminal**.
4. Configurez les paramètres du mode terminal.

   Consultez le tableau 5-11 pour une description des paramètres du mode terminal.
5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur le bouton approprié de la page **Paramètres du mode terminal** pour continuer. Consultez le tableau 5-12 pour une description des boutons de la page Paramètres du mode terminal.

**Tableau 5-11. Paramètres du mode terminal**

| Paramètre | Description |
|---|---|
| **Modification de ligne** | Active ou désactive la modification de ligne. |
| **Contrôle de la suppression** | Sélectionnez l'une des options suivantes :<br>• **iDRAC émet un caractère <retarr.><sp><retarr.> lorsque <retarr.> ou <suppr.> est reçu**.<br>• **iDRAC émet un caractère <suppr.> lorsque <retarr.> ou <suppr.> est reçu**. |
| **Contrôle d'écho** | Active ou désactive l'écho. |
| **Contrôle de l'établissement de liaisons** | Active ou désactive l'établissement de liaisons. |
| **Nouvelle séquence linéaire** | Sélectionnez **Aucun**, **<CR-LF>**, **<NULL>**, **<CR>**, **<LF-CR>** ou **<LF>**. |
| **Saisie d'une nouvelle séquence linéaire** | Sélectionnez **<CR>** ou **<NULL>**. |

**Tableau 5-12. Boutons de la page Paramètres du mode terminal**

| Bouton | Description |
|---|---|
| **Imprimer** | Imprime la page **Paramètres du mode terminal**. |
| **Actualiser** | Actualise la page **Paramètres du mode terminal**. |
| **Retourner à la configuration du port série** | Retournez à la page **Configuration du port série**. |
| **Appliquer les modifications** | Applique les modifications apportées aux paramètres du mode terminal. |

---

# Configuration des paramètres réseau d'iDRAC6

**PRÉCAUTION : Si vous modifiez les paramètres réseau de votre iDRAC6, la connexion réseau en cours risque d'être coupée.**

Configurez les paramètres réseau d'iDRAC6 avec l'un des outils suivants :

- Interface Web : consultez « Configuration du NIC iDRAC6 ».
- CLI RACADM : consultez « cfgLanNetworking ».
- Utilitaire de configuration d'iDRAC6 : consultez « Configuration de votre système pour utiliser un iDRAC6 ».

**REMARQUE :** Pour déployer iDRAC6 dans un environnement Linux, consultez « Installation de la RACADM ».

## Accès à iDRAC6 via un réseau

Une fois iDRAC6 configuré, vous pouvez accéder à distance au système géré en utilisant l'une des interfaces suivantes :

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

Le tableau 5-13 décrit chaque interface iDRAC6.

**Tableau 5-13. Interfaces iDRAC6**

| Interface | Description |
|---|---|
| Interface Web | Fournit un accès à distance à iDRAC6 à l'aide d'une interface utilisateur graphique. L'interface Web est intégrée au micrologiciel iDRAC6 et est accessible via l'interface NIC d'un navigateur Web pris en charge sur la station de gestion. |
| RACADM | Fournit un accès à distance à iDRAC6 à l'aide d'une interface de ligne de commande. La RACADM utilise l'adresse IP d'iDRAC6 pour exécuter les commandes RACADM.<br><br>**REMARQUE :** La capacité à distance de la racadm est prise en charge uniquement sur les stations de gestion. Pour plus d'informations, consultez « Utilisation de la RACADM à distance ».<br><br>**REMARQUE :** Lors de l'utilisation de la capacité à distance de la racadm, vous devez disposer d'un accès en écriture sur les dossiers sur lesquels vous utilisez les sous-commandes RACADM impliquant des opérations sur des fichiers, par exemple :<br><br>`racadm getconfig -f <nom de fichier>`<br><br>ou :<br><br>`sous-commandes racadm sslcertupload -t 1 -f c:\cert\cert.txt` |
| Console Telnet | Donne accès à iDRAC6 et permet la prise en charge des commandes série et la RACADM, y compris les commandes **powerdown**, **powerup**, **powercycle** et **hardreset**.<br><br>**REMARQUE :** Telnet est un protocole non sécurisé qui transmet toutes les données, y compris les mots de passe, en texte simple. Lors de la transmission d'informations critiques, utilisez l'interface SSH. |
| Interface SSH | Fournit les mêmes capacités que la console Telnet en utilisant une couche de transport cryptée pour une sécurité accrue. |
| Interface IPMI | Fournit l'accès via iDRAC6 aux fonctionnalités de gestion de base du système distant. L'interface inclut IPMI sur LAN, IPMI sur communications série et Communications série sur LAN. Pour plus d'informations, consultez le Guide d'utilisation de *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com\manuals**. |

**REMARQUE :** Le nom d'utilisateur par défaut d'iDRAC6 est `root` et le mot de passe par défaut est `calvin`.

Vous pouvez accéder à l'interface Web d'iDRAC6 via le NIC iDRAC6 en utilisant un navigateur Web pris en charge, Server Administrator ou IT Assistant.

Pour accéder à l'interface d'accès à distance d'iDRAC6 avec Server Administrator, procédez comme suit :

- Lancez Server Administrator.
- Dans l'arborescence du système située sur le panneau gauche de la page d'accueil de Server Administrator, cliquez sur **Système** → **Châssis principal du système** → **Remote Access Controller**.

Pour plus d'informations, consultez le *Guide d'utilisation de Server Administrator*.

## Utilisation de la RACADM à distance

**REMARQUE :** Configurez l'adresse IP sur votre iDRAC6 avant d'utiliser la capacité d'accès à distance de la RACADM. Pour plus d'informations sur la configuration de votre iDRAC6 et une liste des documents connexes, consultez « Installation de base d'iDRAC6 ».

La RACADM fournit une option de capacité d'accès à distance (**-r**) qui vous permet de vous connecter au système géré et d'exécuter les sous-commandes RACADM à partir d'une console distante ou d'une station de gestion. Pour utiliser la capacité d'accès à distance, il vous faut un nom d'utilisateur (option **-u**) et un mot de passe (option **-p**) valides, ainsi que l'adresse IP d'iDRAC6.

**REMARQUE :** Si le système depuis lequel vous accédez au système distant ne comporte pas de certificat iDRAC6 dans sa réserve de certificats par défaut, un message apparaît lorsque vous tapez une commande RACADM. Pour plus d'informations sur les certificats iDRAC6, consultez « Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques ».

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.

(Alerte de sécurité : le certificat est invalide : le nom sur le certificat est invalide ou ne correspond pas au nom du site

Continuer l'exécution. Utilisez l'option -S pour que la racadm interrompe l'exécution sur les erreurs liées au certificat.)
```

La RACDMA continue d'exécuter la commande. Toutefois, si vous utilisez l'option –S, la RACADM arrête d'exécuter la commande et affiche le message suivant :

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

(Alerte de sécurité : le certificat est invalide : le nom sur le certificat est invalide ou ne correspond pas au nom du site

racadm interrompt l'exécution de la commande.)
```

ERREUR : impossible de se connecter à iDRAC6 à l'adresse IP spécifiée

## Synopsis de la RACADM

```
racadm -r <adresse IP iDRAC6> -u <nom d'utilisateur> -p <mot de passe> <sous-commande> <options de la sous-commande>

racadm -i -r <adresse IP iDRAC6> <sous-commande> <options de la sous-commande>
```

Par exemple :

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Si le numéro de port HTTPS d'iDRAC6 a été remplacé par un port personnalisé autre que le port par défaut (443), la syntaxe suivante doit être utilisée :

```
racadm -r <adresse IP d'iDRAC6>:<port> -u <nom d'utilisateur> -p <mot de passe> <sous-commande> <options de la sous-commande>

racadm -i -r <adresse IP d'iDRAC6>:<port> <sous-commande> <options de la sous-commande>
```

## Options de la RACADM

Le tableau 5-14 énumère les options de la commande RACADM.

**Tableau 5-14. Options de la commande racadm**

| Option | Description |
|---|---|
| -r <*Adresse_IP_RAC*> | Spécifie l'adresse IP distante du contrôleur. |
| -r <*Adresse_IP_RAC*>:<*numéro de port*> | Utilisez <*numéro de port*> si le numéro de port iDRAC6 n'est pas le port par défaut (443) |
| -i | Ordonne à la RACADM de demander de manière interactive à l'utilisateur son nom d'utilisateur et son mot de passe. |
| -u <*Nom_d'utilisateur*> | Spécifie le nom d'utilisateur qui est utilisé pour authentifier la transaction de commande. Si l'option **-u** est utilisée, l'option **-p** doit être utilisée et l'option **-i** (interactive) n'est pas autorisée. |
| -p <*mot de passe*> | Spécifie le mot de passe utilisé pour authentifier la transaction de commande. Si l'option **-p** est utilisée, l'option **-i** n'est pas autorisée. |
| -S | Indique que la RACADM doit contrôler les erreurs de certificat non valide. La RACADM interrompt l'exécution de la commande avec un message d'erreur si elle détecte un certificat non valide. |

---

# Activation et désactivation de la capacité d'accès à distance de la RACADM

**REMARQUE :** Il est recommandé d'exécuter ces commandes sur votre système local.

Par défaut, la capacité d'accès à distance de la RACADM est activée. Si elle est désactivée, tapez la commande RACADM suivante pour l'activer :

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

Pour désactiver la capacité d'accès à distance, tapez :

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

## Sous-commandes RACADM

Le tableau 5-15 fournit une description de chaque sous-commande RACADM que vous pouvez exécuter dans la RACADM. Pour obtenir une liste détaillée des sous-commandes RACADM, y compris la syntaxe et les entrées valides, consultez « Présentation de la sous-commande RACADM ».

Lorsque vous saisissez une sous-commande RACADM, utilisez comme préfixe de commande racadm, par exemple :

```
racadm help
```

**Tableau 5-15. Sous-commandes RACADM**

| Commande | Description |
|---|---|
| **help** | Répertorie les sous-commandes iDRAC6. |
| **help** *<sous-commande>* | Répertorie les instructions d'utilisation pour la sous-commande spécifiée. |
| **arp** | Affiche le contenu de la table ARP. Les entrées de la table ARP ne peuvent être ni ajoutées, ni supprimées. |
| **clearasrscreen** | Efface l'écran de la dernière panne (dernier écran bleu). |
| **clrraclog** | Efface le journal iDRAC6. Une entrée unique est effectuée pour indiquer l'utilisateur et l'heure à laquelle le journal a été effacé. |
| **config** | Configure iDRAC6. |
| **getconfig** | Affiche les propriétés de configuration iDRAC6 actuelles. |
| **coredump** | Affiche le dernier vidage de mémoire d'iDRAC6. |
| **coredumpdelete** | Supprime le vidage de mémoire stocké sur iDRAC6. |
| **fwupdate** | Exécute ou affiche la condition des mises à jour du micrologiciel iDRAC6. |
| **getssninfo** | Affiche des informations sur les sessions actives. |
| **getsysinfo** | Affiche des informations générales concernant l'iDRAC6 et le système. |
| **getractime** | Affiche l'heure iDRAC6. |
| **ifconfig** | Affiche la configuration IP iDRAC6 actuelle. |
| **netstat** | Affiche la table de routage et les connexions actuelles. |
| **ping** | Vérifie que l'adresse IP de destination est accessible à partir d'iDRAC6 avec le contenu actuel de la table de routage. |
| **setniccfg** | Définit la configuration IP du contrôleur. |
| sshpkauth | Vous permet de téléverser jusqu'à 4 clés publiques SSH différentes, de supprimer des clés existantes et d'afficher les clés déjà présentes dans iDRAC6. |
| **getniccfg** | Affiche la configuration IP actuelle du contrôleur. |
| **getsvctag** | Affiche les numéros de service. |
| **racdump** | Vide les informations de condition et d'état d'iDRAC6 pour le débogage de la mémoire. |
| **racreset** | Réinitialise iDRAC6. |
| **racresetcfg** | Réinitialise la configuration par défaut d'iDRAC6. |
| **serveraction** | Effectue des opérations de gestion de l'alimentation sur le système géré. |
| **getraclog** | Affiche le journal d'iDRAC6. |
| **clrsel** | Efface les entrées du journal des événements système. |
| **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. |
| **sslcsrgen** | Génère et télécharge la RSC SSL. |
| **sslcertupload** | Téléverse un certificat d'AC ou un certificat de serveur vers iDRAC6. |
| **sslcertdownload** | Télécharge un certificat d'AC. |
| **sslcertview** | Affiche un certificat d'AC ou un certificat de serveur dans iDRAC6. |
| **sslkeyupload** | Téléverse la clé SSL du client vers iDRAC6. |
| **testtrap** | Contraint iDRAC6 à envoyer une interruption SNMP test sur le NIC iDRAC6 pour vérifier la configuration de l'interruption. |
| **vmdisconnect** | Force la déconnexion du média virtuel. |
| **vmkey** | Réinitialise la valeur par défaut de la taille du disque flash virtuel (256 Mo). |

## Questions les plus fréquentes sur les messages d'erreur de la RACADM

**Une fois iDRAC6 réinitialisé (avec la commande racadm racreset), j'envoie une commande et le message suivant s'affiche :**

**ERROR: Unable to connect to RAC at specified IP address**

**(ERREUR : impossible de se connecter au RAC à l'adresse  IP spécifiée.)**

**Qu'est-ce que ce message signifie ?**

Vous devez attendre qu'iDRAC6 soit entièrement réinitialisé avant d'émettre une autre commande.

**Lorsque j'utilise les commandes et les sous-commandes racadm, il y a des erreurs que je  ne comprends pas.**

Une ou plusieurs des erreurs suivantes peuvent survenir lorsque vous utilisez les commandes et les sous-commandes RACADM :

- Messages d'erreur de la RACADM locale : problèmes de syntaxe, d'erreurs typographiques et de noms incorrects.
- Messages d'erreur de la RACADM distante : problèmes d'adresse IP incorrecte, de nom d'utilisateur incorrect ou de mot de passe incorrect.

**Lorsque j'utilise ping pour l'adresse IP d'iDRAC6 de mon système, puis commute mon iDRAC6 entre les modes Dédié et Partagé pendant la réponse ping, je ne reçois aucune réponse.**

Effacez la table ARP sur votre système.

---

## Configuration de plusieurs contrôleurs iDRAC6

À l'aide de la RACADM, vous pouvez configurer un ou plusieurs contrôleurs iDRAC6 avec des propriétés identiques. Lorsque vous effectuez une requête sur un contrôleur iDRAC6 spécifique à l'aide de sa référence de groupe et d'objet, la RACADM crée le fichier de configuration **racadm.cfg** à partir des informations récupérées. En exportant le fichier vers un ou plusieurs iDRAC6, vous pouvez configurer vos contrôleurs avec des propriétés identiques en un minimum de temps.

**REMARQUE :** Certains fichiers de configuration contiennent des informations iDRAC6 uniques (comme l'adresse IP statique) qui doivent être modifiées avant d'exporter le fichier vers d'autres iDRAC6.

Pour configurer plusieurs contrôleurs iDRAC6, procédez de la manière suivante :

1. Utilisez la RACADM pour effectuer une requête sur l'iDRAC6 cible qui contient la configuration appropriée.

   **REMARQUE :** Le fichier **.cfg** généré ne contient pas de mots de passe utilisateur.

   Ouvrez une invite de commande et tapez :

   ```
   racadm getconfig -f myfile.cfg
   ```

   **REMARQUE :** La redirection d'une configuration iDRAC6 vers un fichier à l'aide de **getconfig-f** est seulement prise en charge avec les interfaces de la RACADM locale et distante.

2. Modifiez le fichier de configuration à l'aide d'un simple éditeur de texte (optionnel).

3. Utilisez le nouveau fichier de configuration pour modifier un iDRAC6 cible.

   À l'invite de commande, tapez :

   ```
   racadm config –f myfile.cfg
   ```

4. Réinitialisez l'iDRAC6 cible qui a été configuré.

   À l'invite de commande, tapez :

   ```
   racadm racreset
   ```

La sous-commande **getconfig -f racadm.cfg** demande la configuration d'iDRAC6 et génère le fichier **racadm.cfg**. Si nécessaire, vous pouvez configurer le fichier avec un autre nom.

Vous pouvez utiliser la commande **getconfig** pour pouvoir effectuer les actions suivantes :

- afficher toutes les propriétés de configuration dans un groupe (spécifié par le nom de groupe et l'index),
- afficher toutes les propriétés de configuration pour un utilisateur par nom d'utilisateur.

La sous-commande **config** charge les informations dans l'autre iDRAC6. Utilisez **config** pour synchroniser la base de données des utilisateurs et des mots de passe avec Server Administrator.

Le nom du fichier de configuration initial, **racadm.cfg**, est défini par l'utilisateur. Dans l'exemple suivant, le fichier de configuration s'appelle **myfile.cfg**. Pour créer ce fichier, tapez la commande suivante à l'invite de commande :

```
racadm getconfig -f myfile.cfg
```

**PRÉCAUTION : Il est recommandé de modifier ce fichier avec un simple éditeur de texte. L'utilitaire RACADM utilise un analyseur de texte ASCII. Tout formatage peut troubler l'analyseur et ainsi corrompre la base de données de la RACADM.**

## Création d'un fichier de configuration iDRAC6

Le fichier de configuration iDRAC6, **<***nom de fichier***>.cfg,** est utilisé avec la commande `racadm config -f <nom de fichier>.cfg`. Vous pouvez utiliser le fichier

de configuration pour créer un fichier de configuration (similaire à un fichier **.ini**) et configurer iDRAC6 à partir de ce fichier. Vous pouvez utiliser n'importe quel nom de fichier et le fichier ne nécessite pas d'extension **.cfg** (bien qu'il y soit fait référence par ce nom d'extension dans cette sous-section).

Le fichier **.cfg** peut être :

- créé,
- obtenu à partir de la commande `racadm getconfig -f <nom de fichier>.cfg`,
- obtenu à partir de la commande `racadm getconfig -f <nom de fichier>.cfg`, puis modifié.

**REMARQUE :** Consultez « getconfig » pour des informations sur la commande **getconfig**.

Le fichier **.cfg** est d'abord analysé pour vérifier si des noms de groupe et d'objet valides sont présents et si quelques règles de syntaxe simples ont été observées. Les erreurs sont indiquées avec le numéro de ligne dans laquelle l'erreur a été détectée et un message simple explique le problème. Le fichier entier est analysé pour vérifier son exactitude et toutes les erreurs sont affichées. Les commandes d'écriture ne sont pas transmises à iDRAC6 si une erreur est trouvée dans le fichier **.cfg**. L'utilisateur doit corriger *toutes* les erreurs pour que la configuration ait lieu. L'option **-c** peut être utilisée avec la sous-commande **config** qui ne vérifie que la syntaxe et n'effectue *pas* d'opération d'écriture sur iDRAC6.

Suivez les instructions ci-dessous lorsque vous créez un fichier **.cfg :**

- Si l'analyseur rencontre un groupe indexé, c'est la valeur de l'objet ancré qui différencie les différents index.

  L'analyseur lit tous les index d'iDRAC6 pour ce groupe. Les objets présents dans ce groupe sont de simples modifications lorsqu'iDRAC6 est configuré. Si un objet modifié représente un nouvel index, l'index est créé sur l'iDRAC6 au cours de la configuration.

- Vous ne pouvez pas spécifier l'index de votre choix dans un fichier **.cfg**.

  Les index peuvent être créés et supprimés ; ainsi, au fil du temps, 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 d'établir des correspondances d'index exactes entre tous les RAC gérés. Les nouveaux utilisateurs sont ajoutés au premier index disponible. Un fichier **.cfg** qui analyse et s'exécute correctement sur un iDRAC6 peut ne pas s'exécuter correctement sur un autre si tous les index sont remplis et que vous devez ajouter un nouvel utilisateur.

- Utilisez la sous-commande **racresetcfg** pour configurer plusieurs iDRAC6 avec des propriétés identiques.

  Utilisez la sous-commande **racresetcfg** pour réinitialiser iDRAC6 sur ses paramètres initiaux par défaut et exécutez ensuite la commande `racadm config -f <nom de fichier>.cfg`. Le fichier **.cfg** doit inclure tous les objets, utilisateurs, index et autres paramètres requis.

**PRÉCAUTION : Utilisez la sous-commande racresetcfg pour réinitialiser la base de données et les paramètres du NIC iDRAC6 sur les paramètres par défaut d'origine 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 réinitialisés.**

## Règles d'analyse

- Toutes les lignes commençant par « # » sont traitées comme des commentaires.

  Une ligne de commentaire *doit* commencer dans la première colonne. Un caractère « # » dans une autre colonne est traité comme un caractère « # ».

  Certains paramètres de modem peuvent inclure les caractères # dans leur chaîne. Un caractère d'échappement n'est pas exigé. Vous pouvez générer un fichier **.cfg** à partir d'une commande `racadm getconfig -f <nom de fichier>.cfg`, puis exécuter une commande `racadm config -f <nom de fichier>.cfg` sur un autre iDRAC6 sans ajouter de caractères d'échappement.

  **Exemple :**

  ```
  #

  # Il s'agit d'un commentaire

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Init modem # n'est pas un commentaire>
  ```

- Toutes les entrées de groupe doivent être entourées des caractères « **[ »** et « **] »**.

  Le caractère de début « **[ »** indiquant un nom de groupe *doit* commencer dans la première colonne. Ce nom de groupe *doit* être spécifié avant n'importe quel objet dans ce groupe. Les objets auxquels aucun nom de groupe n'est associé génèrent une erreur. Les données de configuration sont organisées en groupes, comme défini dans « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

  L'exemple suivant affiche un nom de groupe, un objet et la valeur de propriété de l'objet.

  **Exemple :**

  ```
  [cfgLanNetworking] - {nom de groupe}

  cfgNicIpAddress=143.154.133.121 {nom d'objet}
  ```

- Tous les paramètres sont spécifiés en tant que paires « objet=valeur » sans espace entre l'objet, le signe = et la valeur.

  Les espaces blancs qui sont inclus après la valeur sont ignorés. Un espace blanc à l'intérieur d'une chaîne de valeurs n'est pas modifié. Les caractères à droite de « = » sont pris tels quels (par exemple, un second « = » ou un « # », « [ », « ] », etc.). Ces caractères sont des caractères de script de conversation de modem valides.

  Consultez l'exemple de la puce précédente.

- L'analyseur **.cfg** ignore une entrée d'objet d'index.

  Vous *ne pouvez pas* spécifier quel index est utilisé. Si l'index existe déjà, il est utilisé ou la nouvelle entrée est créée dans le premier index disponible pour ce groupe.

  La commande `racadm getconfig-f <nom de fichier>.cfg` place un commentaire devant les objets d'index, ce qui permet à l'utilisateur de voir les commentaires inclus.

**REMARQUE :** Vous pouvez créer un groupe indexé manuellement en utilisant la commande suivante :
`racadm config -g <nom de groupe> -o <objet ancré> -i <index 1-16> <nom d'ancre unique>`

- La ligne d'un groupe indexé *ne peut pas* être supprimée d'un fichier **.cfg**.

  Vous devez supprimer un objet indexé manuellement en utilisant la commande suivante :

  ```
  racadm config -g <nom de groupe> -o <nom d'objet> -i <index 1-16> ""
  ```

**REMARQUE :** Une chaîne 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 de groupe> -i <index 1-16>
  ```

- Pour les groupes indexés, l'ancre de l'objet *doit* être le premier objet après la paire « [ ] ». Voici des exemples de groupes indexés actuels :

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<NOM_D'UTILISATEUR>
  ```

  Si vous tapez `racadm getconfig -f <monexample>.cfg`, la commande construit un fichier .cfg pour la configuration iDRAC6 actuelle. Ce fichier de configuration peut être utilisé comme exemple et comme point de départ de votre fichier **.cfg** unique.

## Modification de l'adresse IP iDRAC6

Lorsque vous modifiez l'adresse IP iDRAC6 dans le fichier de configuration, supprimez toutes les entrées **<***variable***>**=**valeur** inutiles. Seul le nom du groupe variable réel avec « [ » et « ] » demeure, avec les deux entrées **<***variable***>**= **valeur** correspondant au changement d'adresse IP.

Par exemple :

```
#

# Groupe d'objet « cfgLanNetworking »

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#

# Groupe d'objet « cfgLanNetworking »

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# commentaire, le reste de cette ligne est ignoré

cfgNicGateway=10.35.9.1
```

La commande **racadm config-f myfile.cfg** analyse le fichier et identifie les erreurs par numéro de ligne. Un fichier correct met à jour les entrées appropriées. En outre, vous pouvez utiliser la même commande **getconfig** utilisée dans l'exemple précédent pour confirmer la mise à jour.

Utilisez ce fichier pour télécharger des modifications à l'échelle de la société ou pour configurer de nouveaux systèmes sur le réseau.

**REMARQUE :** « Ancre » est un terme interne et ne doit pas être utilisé dans le fichier.

## Configuration des propriétés réseau 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 d'iDRAC6 au démarrage lorsque vous êtes invité à taper <Ctrl><E>. Pour plus d'informations sur la configuration des propriétés réseau à l'aide de l'utilitaire de configuration d'iDRAC6, consultez « Configuration de votre système pour utiliser un iDRAC6 ».

L'exemple suivant montre comment la commande peut être utilisée pour configurer les propriétés réseau du LAN souhaitées.

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

**REMARQUE :** Si la commande **cfgNicEnable** est définie sur **0**, le LAN iDRAC6 est désactivé, même si DHCP est activé.

### Modes iDRAC6

iDRAC6 peut être configuré dans l'un des quatre modes :

- Dédié
- Partagé
- Partagé avec basculement LOM2
- Partagé avec basculement tous les LOM

Le tableau 5-16 fournit une description de chaque mode.

**Tableau 5-16. Configurations du NIC iDRAC6**

| Mode | Description |
|---|---|
| Dédié | iDRAC6 utilise son propre NIC (connecteur RJ-45) et l'adresse MAC iDRAC pour le trafic réseau. |
| Partagé | iDRAC6 utilise LOM1 sur le planaire. |
| Partagé avec basculement LOM2 | iDRAC6 utilise LOM1 et LOM2 comme groupe pour le basculement. Le groupe utilise l'adresse MAC iDRAC6. |
| Partagé avec basculement tous les LOM | iDRAC6 utilise LOM1, LOM2, LOM3 et LOM4 comme groupe pour le basculement. Le groupe utilise l'adresse MAC iDRAC6. |

---

## Questions les plus fréquentes concernant la sécurité réseau

**Lorsque j'accède à l'interface Web iDRAC6, un avertissement de sécurité s'affiche et indique que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte d'iDRAC6**.

iDRAC6 est doté d'un certificat de serveur iDRAC6 par défaut qui assure la sécurité du réseau pour l'interface Web et les fonctionnalités de la RACADM distante. Lorsque ce certificat est utilisé, le navigateur Web affiche un avertissement de sécurité, car le certificat par défaut est émis sur le **certificat par défaut iDRAC6**, lequel ne correspond pas au nom d'hôte d'iDRAC6 (l'adresse IP, par exemple).

Pour résoudre ce problème de sécurité, téléversez un certificat de serveur iDRAC6 émis sur l'adresse IP ou le nom iDRAC d'iDRAC6. Lors de la génération d'une requête de signature de certificat (RSC) utilisée pour émettre le certificat, assurez-vous que le nom commun (NC) de la RSC correspond à l'adresse IP (**si le certificat est émis sur IP**) iDRAC6 (par exemple, 192.168.0.120) ou au nom iDRAC6 DNS enregistré (**si le certificat est émis au nom enregistré d'iDRAC**).

Afin de vous assurer que la RSC corresponde bien au nom iDRAC6 DNS enregistré :

1. Dans l'arborescence du **système**, cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Réseau**.
3. Dans le tableau **Paramètres communs :**
   a. Sélectionnez la case à cocher **Enregistrer iDRAC sur DNS**.
   b. Dans le champ **Nom IDRAC DNS**, saisissez le nom d'iDRAC6.
4. Cliquez sur **Appliquer les modifications**.

Consultez « Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques » pour plus d'informations sur la génération de RSC et l'émission de certificats.

**RACADM distante et les services Web ne sont plus disponibles lorsque les propriétés sont modifiées. Pourquoi ?**

Lorsque vous réinitialisez le serveur Web iDRAC6, il peut s'écouler un certain temps avant que les services de la RACADM distante et l'interface Web ne redeviennent disponibles.

Le serveur Web iDRAC6 est réinitialisé dans les cas suivants :

- quand les propriétés de configuration réseau ou de sécurité réseau sont modifiées à l'aide de l'interface utilisateur Web d'iDRAC6,
- quand la propriété **cfgRacTuneHttpsPort** est modifiée (y compris lorsqu'une commande config -f <*fichier config*> la modifie),
- quand on utilise **racresetcfg,**
- quand iDRAC6 est réinitialisé,
- quand un nouveau certificat de serveur SSL est téléversé.

**Mon serveur DNS n'enregistre pas mon iDRAC6. Pourquoi ?**

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

**Lorsque j'accède à l'interface Web iDRAC6, un avertissement de sécurité s'affiche ; il m'informe que le certificat SSL a été émis par une autorité de certification (AC) qui n'est pas fiable.**

iDRAC6 est doté d'un certificat de serveur iDRAC6 par défaut qui assure la sécurité du réseau pour l'interface Web et les fonctionnalités de la RACADM distante. Ce certificat n'a pas été émis par une AC de confiance. Pour résoudre ce problème de sécurité, téléversez un certificat de serveur iDRAC6 émis par une AC de confiance (Microsoft Certificate Authority, Thawte ou Verisign, par exemple). Consultez « Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques » pour obtenir de plus amples informations sur l'émission de certificats.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Ajout et configuration d'utilisateurs iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Pour gérer votre système avec iDRAC6 et maintenir la sécurité du système, créez des utilisateurs uniques avec des droits d'administrateur spécifiques (ou *autorité basée sur les rôles*). Pour une sécurité supplémentaire, vous pouvez aussi configurer des alertes qui sont envoyées par e-mail à des utilisateurs spécifiques quand un événement système spécifique se produit.

---

## Utilisation de l'interface Web pour configurer des utilisateurs iDRAC6

### Ajout et configuration d'utilisateurs iDRAC6

Pour gérer votre système avec iDRAC6 et maintenir la sécurité du système, créez des utilisateurs uniques avec des droits d'administrateur spécifiques (ou *autorité basée sur les rôles*).

Pour ajouter et configurer des utilisateurs iDRAC6, effectuez les étapes suivantes :

**REMARQUE :** Vous devez disposer du droit **Configurer des utilisateurs** pour configurer un utilisateur iDRAC.

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

   **La page Utilisateurs** (consultez le tableau 6-1) affiche les informations suivantes pour les utilisateurs iDRAC6 : **Référence utilisateur, État (Activé/Désactivé), Nom d'utilisateur, Privilèges RAC**, **Privilèges utilisateur sur LAN**, **Privilèges utilisateur sur port série** et **Privilèges des communications série sur LAN (Activé/Désactivé)**.

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

2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.

   Sur la page **Menu principal utilisateur** (consultez le tableau 6-2 et le tableau 6-8), vous pouvez configurer un utilisateur, afficher ou téléverser un certificat d'utilisateur, téléverser un certificat d'une autorité de certification (AC) de confiance, afficher un certificat d'une AC de confiance, téléverser un fichier de clé publique SSH (Secure Shell) ou afficher ou supprimer une clé SSH spécifiée ou toutes les clés SSH.

   Si vous sélectionnez **Configurer l'utilisateur** et cliquez sur **Suivant**, la page **Configuration de l'utilisateur** apparaît.

3. Dans la page **Configuration de l'utilisateur**, configurez les éléments suivants :
   - Nom d'utilisateur, mot de passe et droits d'accès pour un nouvel utilisateur iDRAC ou un utilisateur iDRAC existant. Le tableau 6-3 décrit les **Paramètres généraux de l'utilisateur**.
   - Les privilèges IPMI de l'utilisateur. Le tableau 6-4 décrit les **Privilèges d'utilisateur IPMI** pour la configuration des privilèges LAN de l'utilisateur.
   - Les privilèges d'utilisateur iDRAC. Le tableau 6-5 décrit les **Privilèges d'utilisateur iDRAC**.
   - Les droits d'accès du groupe iDRAC. Le tableau 6-6 décrit les **Droits d'accès du groupe iDRAC**.

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

5. Cliquez sur le bouton approprié pour continuer. Consultez le tableau 6-7.

**Tableau 6-1. États et droits d'utilisateur**

| Paramètre | Description |
|---|---|
| **Réf. utilisateur** | Affiche la liste séquentielle des numéros de référence utilisateur. Chaque champ sous **Réf. utilisateur** contient l'un des 16 numéros de référence utilisateur prédéfinis. Ce champ ne peut pas être modifié. |
| **État** | Affiche l'état d'ouverture de session de l'utilisateur : Activé ou Désactivé. (Désactivé est la valeur par défaut.)<br><br>**REMARQUE :** L'utilisateur 2 est activé par défaut. |
| **Nom d'utilisateur** | Affiche le nom d'ouverture de session de l'utilisateur. Spécifie un nom d'utilisateur iDRAC6 contenant jusqu'à 16 caractères. Chaque utilisateur doit avoir un nom d'utilisateur unique.<br><br>**REMARQUE :** Les noms d'utilisateur sur iDRAC6 ne doivent pas contenir de caractères non pris en charge tels que les caractères « **/** » (barre oblique), « **** » (barre oblique inversée), « **.** » (point) et **@**. L'espace ainsi que les autres caractères |

| | |
|---|---|
| | sont autorisés, mais l'espace blanc ne l'est pas.<br><br>**REMARQUE :** Si le nom d'utilisateur est modifié, le nouveau nom n'apparaît pas dans l'interface utilisateur jusqu'à la prochaine ouverture de session utilisateur. |
| **Privilège du RAC** | Définit le groupe (niveau de privilège) auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun). |
| **Privilèges utilisateur sur LAN** | Affiche le niveau de privilège LAN IPMI auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun). |
| **Privilèges utilisateur sur port série** | Affiche le niveau de privilège de port série IPMI auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun). |
| **Privilèges des communications série sur LAN** | Permet/Interdit à l'utilisateur d'utiliser les communications série sur LAN IPMI. |

**Tableau 6-2. Options de configuration de la carte à puce**

| Option | Description |
|---|---|
| **Téléverser le certificat d'utilisateur** | Permet à l'utilisateur de téléverser le certificat d'utilisateur vers iDRAC6 et de l'importer dans le profil utilisateur. |
| **Consulter le certificat de l'utilisateur** | Affiche la page Certificat de l'utilisateur qui a été téléversée vers iDRAC. |
| **Téléverser le certificat d'une AC de confiance** | Vous permet de téléverser le certificat d'une AC de confiance sur iDRAC et de l'importer dans le profil utilisateur. |
| **Afficher le certificat d'une AC de confiance** | Affiche le certificat d'une AC de confiance qui a été téléversé vers iDRAC. Le certificat d'une AC de confiance est émis par l'AC qui est autorisée à émettre des certificats aux utilisateurs. |

**Tableau 6-3. Paramètres généraux de l'utilisateur**

| | |
|---|---|
| Réf. utilisateur | Un des 16 numéros de référence utilisateur prédéfinis. |
| **Activer l'utilisateur** | Lorsqu'elle est cochée, cette case indique que l'accès de l'utilisateur à iDRAC6 est activé. Lorsqu'elle est décochée, l'accès utilisateur est désactivé. |
| **Nom d'utilisateur** | Nom d'utilisateur comportant jusqu'à 16 caractères. |
| **Modifier le mot de passe** | Active les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. Lorsque cette option n'est pas cochée, le **mot de passe** de l'utilisateur ne peut pas être modifié. |
| **Nouveau mot de passe** | Saisissez un **mot de passe** de 20 caractères maximum. Les caractères ne sont pas affichés. |
| **Confirmer le nouveau mot de passe** | Retapez le mot de passe de l'utilisateur iDRAC pour le confirmer. |

**Tableau 6-3. Privilèges d'utilisateur IPMI**

| Propriété | Description |
|---|---|
| **Privilège maximal 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 : **Administrateur**, **Opérateur**, **Utilisateur ou Aucun**. |
| **Privilège maximal de l'utilisateur accordé sur le port série** | Spécifie le privilège maximal de l'utilisateur sur le canal série IPMI sur l'un des groupes d'utilisateurs suivants : **Administrateur**, **Opérateur**, **Utilisateur ou Aucun**. |
| **Activation des communications série sur LAN** | Permet à l'utilisateur d'utiliser les communications série sur LAN IPMI. Lorsque cette option est cochée, ce privilège est activé. |

**Tableau 6-5. Privilèges utilisateur iDRAC**

| Propriété | Description |
|---|---|
| **Rôles** | Spécifie le privilège maximal d'utilisateur iDRAC de l'utilisateur sur l'un des privilèges suivants : **Administrateur**, **Opérateur**, **Lecture seule** ou **Aucun**. Consultez le tableau 6-6 pour connaître les **Droits du groupe iDRAC**. |
| **Ouvrir une session sur iDRAC** | Permet à l'utilisateur d'ouvrir une session sur iDRAC. |
| **Configurer iDRAC** | Permet à l'utilisateur de configurer iDRAC. |
| **Configurer les utilisateurs** | Permet à l'utilisateur de permettre à des utilisateurs spécifiques d'accéder au système. |
| **Effacer les journaux** | Permet à l'utilisateur d'effacer les journaux iDRAC. |
| **Exécuter les commandes de contrôle du serveur** | Permet à l'utilisateur d'exécuter des commandes de contrôle du serveur. |
| **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. |

| | |
|---|---|
| **Alertes test** | Permet à l'utilisateur d'envoyer des alertes test (par e-mail et PET) à un utilisateur spécifique. |
| **Exécuter des commandes de diagnostic** | Permet à l'utilisateur d'exécuter des commandes de diagnostic. |

**Tableau 6-6. Droits du groupe iDRAC**

| Groupe d'utilisateurs | Droits accordés |
|---|---|
| **Administrateur** | **Ouvrir une session sur iDRAC**, **Configurer iDRAC**, **Configurer des utilisateurs**, **Effacer les journaux**, **Exécuter des commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Alertes test**, **Exécuter des commandes de diagnostic** |
| **Opérateur** | Sélectionne parmi les droits suivants : **Ouvrir une session iDRAC**, **Configurer iDRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter des commandes d'action du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Alertes test**, **Exécuter des commandes de diagnostic** |
| **Lecture seule** | **Ouvrir une session sur iDRAC** |
| **Aucun** | Aucun droit attribué |

**Tableau 6-7. Boutons de la page Configuration de l'utilisateur**

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

## Authentification par clé publique sur SSH

iDRAC6 prend en charge l'authentification par clé publique (PKA) sur SSH. Cette méthode d'authentification améliore l'automatisation avec script SSH en éliminant la nécessité d'intégrer ou de demander la réf. utilisateur/le mot de passe.

### Avant de commencer

Vous pouvez configurer jusqu'à 4 clés publiques *par utilisateur* qui peuvent être utilisées sur une interface SSH. Avant d'ajouter ou de supprimer des clés publiques, veillez à utiliser la commande view pour voir les clés qui sont déjà configurées afin de ne pas écraser ou supprimer une clé accidentellement. Lorsque PKA sur SSH est configuré et utilisé correctement, vous n'avez pas à saisir le nom d'utilisateur ou le mot de passe lorsque vous ouvrez une session sur iDRAC6. Ceci peut s'avérer très utile pour configurer des scripts automatisés pour exécuter diverses fonctions.

Lorsque vous êtes prêt à configurer cette fonctionnalité, tenez compte des points suivants :

- Vous pouvez gérer cette fonctionnalité à l'aide de la RACADM et également depuis l'IUG.
- Lorsque vous ajoutez des clés publiques, vérifiez que les clés existantes ne figurent pas déjà dans l'index dans lequel la nouvelle clé est ajoutée. iDRAC6 n'effectue aucun contrôle pour vérifier que les clés précédentes sont bien supprimées avant l'ajout d'une nouvelle clé. Dès qu'une nouvelle clé est ajoutée, elle est automatiquement effective tant que l'interface SSH est activée.

### Génération de clés publiques pour Windows

Avant d'ajouter un compte, le système qui accèdera à iDRAC6 sur SSH nécessite une clé publique. Deux méthodes sont possibles pour générer la paire de clés publique/privée : utiliser l'application *PuTTY Key Generator* pour les clients exécutant Windows ou la CLI *ssh-keygen* pour les clients exécutant Linux. L'utilitaire de la CLI *ssh-keygen* est disponible par défaut sur toutes les installations standard.

Cette section donne des instructions simples pour générer une paire de clés publique/privée pour les deux applications. Pour une utilisation supplémentaire ou avancée de ces outils, consultez l'Aide de l'application.

Pour utiliser *PuTTY Key Generator* pour les clients Windows afin de créer la clé de base :

1. Démarrez l'application et sélectionnez SSH-2 RSA ou SSH-2 DSA comme type de clé à générer. (SSH-1 n'est pas pris en charge.)
2. RSA et DSA sont les seuls algorithmes de génération de clé pris en charge. Saisissez le nombre de bits de la clé. Ce nombre doit être compris entre 768 et 4 096 bits pour RSA et 1 024 bits pour DSA.
3. Cliquez sur **Générer** et déplacez la souris dans la fenêtre en suivant les instructions. Une fois la clé créée, vous pouvez modifier le champ Commentaire de la clé. Vous pouvez également saisir une phrase de passe pour sécuriser la clé. Veillez à bien enregistrer la clé privée.
4. Vous pouvez enregistrer la clé publique dans un fichier à l'aide de l'option « Enregistrer la clé publique » en vue de son téléversement ultérieur. Toutes les clés téléversées doivent être au format RFC 4716. Si ce n'est pas le cas, vous devez les convertir dans ce format.

### Génération de clés publiques pour Linux

L'application *ssh-keygen* pour les clients Linux est un outil de ligne de commande sans interface utilisateur graphique.

Ouvrez une fenêtre de terminal et saisissez, à l'invite shell :

```
ssh-keygen –t rsa –b 1024 –C testing
```

**REMARQUE :** Les options sont sensibles à la casse.

où

l'option **-t** peut être *dsa* ou *rsa*.

l'option **-b** spécifie la taille du cryptage binaire entre 768 et 4 096.

l'option **-C** permet de modifier le commentaire de la clé publique et est facultative.

Suivez les instructions. Une fois la commande exécutée, téléversez le fichier public.

**PRÉCAUTION : Les clés générées à partir de Linux Management Station avec ssh-keygen ne sont pas au format 4716. Convertissez les clés au format 4716 via `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Ne modifiez pas les droits du fichier de clé. La conversion ci-dessus doit être effectuée à l'aide des droits par défaut.**

**REMARQUE :** iDRAC6 ne prend pas en charge le transfert des clés via ssh-agent.

### Ouverture de session avec l'authentification par clé publique

Une fois les clés publiques téléversées, vous pouvez ouvrir une session sur iDRAC6 sur SSH sans saisir de mot de passe. Vous avez également la possibilité d'envoyer une commande RACADM unique en tant qu'argument de ligne de commande à l'application SSH. Les options de ligne de commande se comportent comme la RACADM distante, car la session se termine une fois la commande exécutée.

Par exemple :

**Ouverture de session :**

```
ssh username@<domaine>
```

ou

```
ssh username@<adresse_IP>
```

où adresse_IP correspond à l'adresse IP d'iDRAC6.

**Envoi de commandes racadm :**

```
ssh username@<domaine> racadm getversion

ssh username@<domaine> racadm getsel
```

## Téléversement, affichage et suppression de clés SSH avec l'interface Web iDRAC6

1. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**→ **Utilisateurs**. La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur. La page **Menu principal utilisateur** s'affiche.
3. Utilisez les options **Configurations de clé SSH** pour téléverser, afficher ou supprimer une ou des clés SSH.

**Tableau 6-8. Configurations de clé SSH**

| Option | Description |
|---|---|
| **Téléverser une ou des clés SSH** | Permet à l'utilisateur local de téléverser un fichier de clé publique SSH (Secure Shell). Si une clé est téléversée, le contenu du fichier de clé s'affiche dans une zone de texte non modifiable de la page **Configuration de l'utilisateur**. |
| **Afficher/Supprimer une ou des clés SSH** | Permet à l'utilisateur local d'afficher ou de supprimer une clé SSH spécifiée ou toutes les clés SSH. |

La page **Téléverser une ou des clés SSH** vous permet de téléverser un fichier de clé publique SSH (Secure Shell). Si une clé est téléversée, le contenu du fichier de clé s'affiche dans une zone de texte non modifiable sur la page **Afficher/Supprimer une ou des clés SSH**

**Tableau 6-9. Téléverser une ou des clés SSH**

| | |
|---|---|

| Option | Description |
|---|---|
| **Fichier/Texte** | Sélectionnez l'option **Fichier** et tapez le chemin de l'emplacement de la clé. Vous pouvez également sélectionner l'option **Texte** et coller le contenu du fichier de clé dans la zone. Vous pouvez téléverser de nouvelles clés ou écraser des clés existantes. Pour téléverser un fichier de clé, cliquez sur **Parcourir**, sélectionnez le fichier, puis cliquez sur le bouton **Appliquer**. |
| **Parcourir** | Cliquez sur ce bouton pour identifier le chemin complet et le nom de fichier de la clé. |

La page **Afficher/Supprimer une ou des clés SSH** vous permet d'afficher ou de supprimer les clés publiques SSH de l'utilisateur.

**Tableau 6-10. Afficher/Supprimer une ou des clés SSH**

| Option | Description |
|---|---|
| **Supprimer** | La clé téléversée s'affiche dans la zone. Sélectionnez l'option Supprimer et cliquez sur **Appliquer** pour supprimer la clé existante. |

## Téléversement, affichage et suppression de clés SSH avec la RACADM

**Téléverser**

Le mode Téléversement vous permet de téléverser un fichier de clé ou de copier le texte de clé sur la ligne de commande. Vous ne pouvez pas téléverser et copier une clé simultanément.

*RACADM locale et RACADM distante :*

```
racadm sshpkauth -i <2 à 16> -k <1 à 4> -f <nom de fichier>
```

*RACADM telnet/ssh/série :*

```
racadm sshpkauth -i <2 à 16> -k <1 à 4> -t

<texte de clé>
```

*Exemple :*

Téléversez une clé valide sur l'utilisateur 2 d'iDRAC6 dans l'espace de la première clé à l'aide d'un fichier :

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

Le fichier de clé d'authentification SSH PK est téléversé avec succès vers le RAC.

**PRÉCAUTION : L'option « texte de clé » n'est pas prise en charge sur la RACADM locale et distante. L'option « fichier » n'est pas prise en charge sur la RACADM Telnet/ssh/série.**

**Affichage**

Le mode Affichage permet à l'utilisateur d'afficher une clé spécifiée par l'utilisateur ou toutes les clés.

```
racadm sshpkauth -i <2 à 16> -v -k <1 à 4>

racadm sshpkauth -i <2 à 16> -v -k all
```

**Suppression**

Le mode Suppression permet à l'utilisateur de supprimer une clé spécifiée par l'utilisateur ou toutes les clés.

```
racadm sshpkauth -i <2 à 16> -d -k <1 à 4>

racadm sshpkauth -i <2 à 16> -d -k all
```

Consultez « sshpkauth » pour obtenir des informations sur les options de la sous-commande.

---

# Utilisation de l'utilitaire de la RACADM pour configurer les utilisateurs iDRAC6

**REMARQUE :** Vous devez avoir ouvert une session en tant qu'utilisateur **root** pour exécuter les commandes RACADM sur un système Linux distant.

Un seul ou plusieurs utilisateurs iDRAC6 peuvent être configurés avec la ligne de commande RACADM installée avec les agents iDRAC6 sur le système géré.

Pour configurer plusieurs iDRAC6 avec des paramètres de configuration identiques, effectuez l'une des procédures suivantes :

- Utilisez les exemples de RACADM indiqués dans cette section comme guide pour créer un fichier séquentiel de commandes RACADM, puis exécutez le fichier séquentiel sur chaque système géré.
- Créez le fichier de configuration iDRAC6 comme décrit dans « Présentation de la sous-commande RACADM » et exécutez la sous-commande **racadm config** sur chaque système géré avec le même fichier de configuration.

## Avant de commencer

Vous pouvez configurer jusqu'à 16 utilisateurs dans la base de données de propriétés iDRAC6. Avant d'activer manuellement un utilisateur iDRAC6, vérifiez s'il existe des utilisateurs actuels. Si vous configurez un nouvel iDRAC6 ou si vous avez exécuté la commande **racadm racresetcfg**, le seul utilisateur actuel est root avec le mot de passe calvin. La sous-commande **racresetcfg** réinitialise les valeurs par défaut d'origine d'iDRAC6.

**PRÉCAUTION : Soyez prudent lorsque vous utilisez la commande racresetcfg, car les valeurs par défaut de *tous* les paramètres de configuration sont réinitialisées. Toute modification précédente est perdue.**

**REMARQUE :** Les utilisateurs peuvent être activés et désactivés à tout moment. Par conséquent, un utilisateur peut avoir un numéro d'index différent sur chaque iDRAC6.

Pour déterminer si un utilisateur existe, tapez la commande suivante à l'invite de commande :

```
racadm getconfig -u <nom d'utilisateur>
```

OU

tapez la commande suivante une fois pour chaque index de 1 à 16 :

```
racadm getconfig -g cfgUserAdmin -i <index>
```

**REMARQUE :** Vous pouvez également taper racadm getconfig -f <monfichier.cfg> et afficher ou modifier le fichier **monfichier.cfg** qui contient tous les paramètres de configuration d'iDRAC6.

Plusieurs paramètres et références d'objet sont affichés avec leurs valeurs actuelles. Les deux objets d'intérêt sont :

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

Si l'objet **cfgUserAdminUserName** n'a pas de valeur, ce numéro d'index, indiqué par l'objet **cfgUserAdminIndex**, peut être utilisé. Si un nom suit le signe « = », cet index est pris par ce nom d'utilisateur.

**REMARQUE :** Lorsque vous activez ou désactivez manuellement un utilisateur avec la sous-commande **racadm config**, vous *devez* spécifier l'index avec l'option **-i**. L'objet **cfgUserAdminIndex** affiché dans l'exemple précédent contient un caractère « # ». De même, si vous utilisez la commande **racadm config -f racadm.cfg** pour spécifier un nombre quelconque de groupes/d'objets à écrire, l'index ne peut pas être spécifié. Un nouvel utilisateur est ajouté au premier index disponible. Ce comportement permet une plus grande flexibilité pour configurer plusieurs iDRAC6 avec les mêmes paramètres.

## Ajout d'un utilisateur iDRAC6

Pour ajouter un nouvel utilisateur à la configuration du RAC, quelques commandes de base peuvent être utilisées. En général, effectuez les procédures suivantes :

1. Définissez le nom d'utilisateur.
2. Définissez le mot de passe.
3. Spécifiez les privilèges d'utilisateur suivants :
   - Privilèges du RAC
   - Privilèges utilisateur sur LAN
   - Privilèges utilisateur sur port série
   - Privilège des communications série sur LAN
4. Activez l'utilisateur.

### Exemple

L'exemple suivant décrit comment ajouter un nouvel utilisateur appelé « John » avec un mot de passe « 123456 » et des privilèges d'ouverture de session au RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminSolEnable 1
```

```
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Pour vérifier, utilisez l'une des commandes suivantes :

```
racadm getconfig -u john
```

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

## Suppression d'un utilisateur iDRAC6

Lorsque vous utilisez la RACADM, les utilisateurs doivent être désactivés manuellement et individuellement. Les utilisateurs ne peuvent pas être supprimés à l'aide d'un fichier de configuration.

L'exemple suivant illustre la syntaxe de commande qui peut être utilisée pour supprimer un utilisateur iDRAC6 :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index> ""
```

Une chaîne de guillemets nulle ("") donne l'ordre à iDRAC6 de supprimer la configuration de l'utilisateur à l'index indiqué et de réinitialiser les valeurs d'usine d'origine de la configuration de l'utilisateur.

## Activation d'un utilisateur iDRAC6 avec des droits

Pour activer un utilisateur avec des droits d'administrateur spécifiques (autorité basée sur les rôles), localisez tout d'abord un index utilisateur disponible en effectuant les étapes dans « Avant de commencer ». Tapez ensuite les lignes de commande suivantes avec le nouveau nom d'utilisateur et le nouveau mot de passe.

**REMARQUE :** Consultez le tableau B-2 pour une liste des valeurs de masque binaire valides correspondant à des privilèges d'utilisateur spécifiques. La valeur de privilège par défaut est 0, qui indique que l'utilisateur n'a aucun privilège activé.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <valeur de masque binaire du privilège d'utilisateur>
```

---

Retour à la page du sommaire

Retour à la page du sommaire

# Utilisation du service de répertoire iDRAC6

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Un service de répertoire permet de maintenir une base de données commune afin d'y stocker des informations concernant les utilisateurs, les ordinateurs, les imprimantes, etc. d'un réseau. Si votre société utilise le logiciel Microsoft® Active Directory® ou le logiciel de service de répertoire LDAP, vous pouvez le configurer pour accéder à iDRAC6, ce qui vous permet d'ajouter et de contrôler les privilèges utilisateur iDRAC6 pour les utilisateurs existants au sein de votre service de répertoire.

---

## Utilisation d'iDRAC6 avec Microsoft Active Directory

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

Le tableau 7-1 affiche les privilèges utilisateur Active Directory iDRAC6.

**Tableau 7-1. Privilèges utilisateur iDRAC6**

| Privilège | Description |
|---|---|
| Ouvrir une session sur iDRAC | Permet à l'utilisateur d'ouvrir une session sur 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 |
| Alertes test | Permet à l'utilisateur d'envoyer des alertes test (par e-mail et PET) à un utilisateur spécifique |
| Exécuter des commandes de diagnostic | Permet à l'utilisateur d'exécuter des commandes de diagnostic |

---

## Spécifications pour l'activation de l'authentification Active Directory pour l'iDRAC6

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

iDRAC6 utilise le mécanisme d'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 de Microsoft pour plus d'informations sur la configuration de PKI.

Pour vous authentifier correctement sur tous les contrôleurs de domaine, vous devez également activer Secure Socket Layer (SSL) sur tous les contrôleurs de domaine auxquels se connecte iDRAC6. Pour des informations plus spécifiques, consultez « Activation de SSL sur un contrôleur de domaine ».

---

## Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur sur iDRAC6 au moyen 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. Ou vous pouvez utiliser la solution de *schéma standard* qui utilise uniquement les objets du groupe Active Directory. Consultez les sections suivantes pour plus d'informations sur ces solutions.

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

La solution de schéma étendu présente les avantages suivants :

- Tous les objets de contrôle d'accès sont maintenus dans Active Directory.
- La configuration de l'accès utilisateur sur différents iDRAC6 dont les niveaux de privilèges diffèrent est assurée.

La solution de schéma standard comporte l'avantage suivant : aucune extension de schéma n'est nécessaire, car toutes les classes d'objets nécessaires sont

fournies par la configuration par défaut de Microsoft du schéma Active Directory.

---

# Présentation d'Active Directory avec le schéma étendu

L'utilisation de la solution de schéma étendu nécessite l'extension de schéma Active Directory, comme indiqué dans la section suivante.

## Extension du schéma Active Directory

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

**REMARQUE :** L'extension du nouveau schéma ou l'installation de la nouvelle extension sur le snap-in Utilisateurs et ordinateurs Active Directory n'a aucun impact sur les produits précédents.

Schema Extender et l'extension snap-in Utilisateurs et ordinateurs Active Directory de la MMC sont disponibles sur le DVD *Dell Systems Management Tools and Documentation*. Pour plus d'informations, consultez « Extension du schéma Active Directory » et « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory ». Pour plus de détails sur l'extension du schéma pour iDRAC6 et l'installation du snap-in Utilisateurs et ordinateurs d'Active Directory de la MMC, consultez le *Guide d'installation et de sécurité de Dell OpenManage* disponible à l'adresse **support.dell.com / manuals**.

**REMARQUE :** Lorsque vous créez des objets Association iDRAC ou des objets Périphérique iDRAC, assurez-vous de sélectionner **Objet avancé Gestion à distance Dell**.

## Extensions de schéma Active Directory

Les données d'Active Directory constituent une base de données distribuée d'attributs et de classes. Le schéma Active Directory inclut les règles qui déterminent le type de données pouvant être ajoutées ou incluses dans la base de données. La classe d'utilisateur est un exemple de classe qui est stockée 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 Active Directory existant peut être défini par une référence unique. Pour que les références soient uniques dans toute l'industrie, Microsoft maintient une base de données d'identifiants d'objets (OID) Active Directory de sorte que lorsque des sociétés ajoutent des extensions au schéma, elles sont sûres que ces extensions sont uniques et ne créent pas de conflits entre elles. Pour étendre le schéma dans Microsoft Active Directory, Dell a reçu des OID uniques, des extensions de noms uniques et des références d'attributs liées de manière unique 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 références des liens du RAC est : 12070 à 12079

## Présentation des extensions de schéma d'iDRAC

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

## Aperçu des objets Active Directory

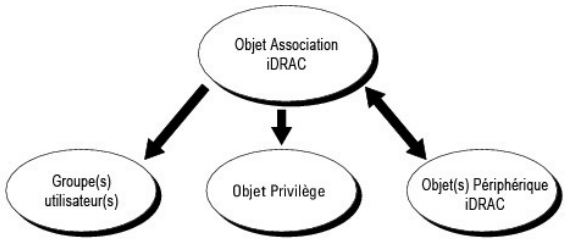
Pour chacun des iDRAC physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, créez au moins un objet Association et un objet Périphérique iDRAC. Vous pouvez créer plusieurs objets Association et chaque objet Association peut être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

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

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

La figure 7-1 illustre le fait que l'objet Association fournit la connexion nécessaire pour toute authentification et autorisation.

**Figure 7-1. Configuration type pour les objets Active Directory**




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

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

L'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory de la MMC permet seulement l'association de l'objet Privilège et des objets iDRAC du même domaine avec l'objet Association. L'extension Dell ne permet pas l'ajout d'un groupe ou d'un objet iDRAC d'autres domaines en tant que membre produit de l'objet Association.

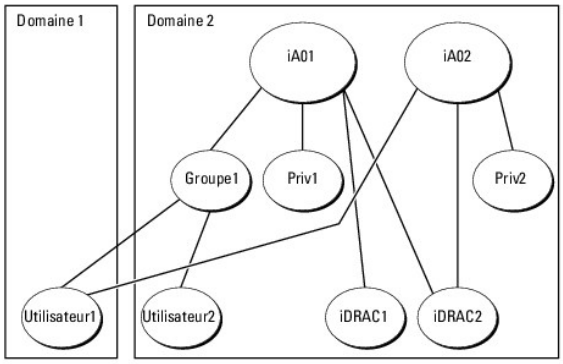
Les utilisateurs, groupes d'utilisateurs ou groupes d'utilisateurs imbriqués depuis tout domaine peuvent être ajoutés dans l'objet Association. Les solutions de schéma étendu prennent en charge tout type de groupe d'utilisateurs et toute imbrication de groupes d'utilisateurs à travers plusieurs domaines autorisés par Microsoft Active Directory.

## Accumulation de privilèges à l'aide du schéma étendu

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

La figure 7-2 fournit un exemple d'accumulation de privilèges à l'aide du schéma étendu.

**Figure 7-2. Accumulation de privilèges pour un utilisateur**




La figure montre deux objets Association : iA01 et iA02. Utilisateur1 est associé à 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 Privr2 a les privilèges Ouvrir une session sur iDRAC, Configurer iDRAC et Alertes test. Par conséquent, Utilisateur1 a maintenant l'ensemble des privilèges Ouvrir une session sur iDRAC, Média virtuel, Effacer les journaux, Configurer iDRAC et Alertes test, 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 maximal de privilèges possibles, en tenant compte des privilèges attribués des différents objets Privilège associés au même utilisateur.

Dans cette configuration, Utilisateur1 possède les privilèges Priv1 et Priv2 sur iDRAC2. Utilisateur1 possède seulement les privilèges Priv1 sur iDRAC1. Utilisateur2 possède les privilèges Priv1 sur iDRAC1 et iDRAC2. En outre, cette figure illustre que Utilisateur1 peut être dans un domaine différent et être associé par un groupe imbriqué.

## Configuration du schéma étendu d'Active Directory pour accéder à votre iDRAC

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

1. Étendez le schéma Active Directory (consultez « Extension du schéma Active Directory »).
2. Étendez le snap-in Utilisateurs et ordinateurs Active Directory (consultez « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Microsoft Active Directory »).

3. Ajoutez des utilisateurs iDRAC6 et leurs privilèges à Active Directory (consultez « Ajout d'utilisateurs iDRAC et de leurs privilèges à Microsoft Active Directory »).

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

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

En étendant votre schéma Active Directory, vous ajoutez une division opérationnelle Dell, des classes et des attributs de schéma, et des exemples d'objets Privilège et Association au schéma Active Directory. Pour étendre le schéma, vous devez avoir des privilèges Administrateur de schéma pour le propriétaire de rôle FSMO (Flexible Single Master Operation) de maître 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, la division opérationnelle Dell ne sera pas ajoutée au schéma.

Les fichiers LDIF et Dell Schema Extender se trouvent 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**

**REMARQUE :** Le dossier **Remote_Management** est dédié à l'extension du schéma sur les produits d'accès à distance antérieurs tels que DRAC 4 et DRAC 5, tandis que le dossier **Remote_Management_Advanced** est dédié à l'extension du schéma sur iDRAC6.

Pour utiliser les fichiers LDIF, consultez les 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, consultez « Utilisation de Dell Schema Extender ».

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

## Utilisation de Dell Schema Extender

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

1. Dans l'écran **Bienvenue**, cliquez sur **Suivant**.

2. Lisez et comprenez 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 MMC et le snap-in du schéma Active Directory pour vérifier ce qui suit :

   - Classes (consultez le tableau 7-2 à le tableau 7-7)
   - Attributs (tableau 7-8)

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

**Tableau 7-2. Définitions de classe pour les classes ajoutées au schéma Active Directory**

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

**Tableau 7-3. Classe dellRacDevice**

| | |
|---|---|
| **OID** | **1.2.840.113556.1.8000.1280.1.7.1.1** |

| | |
|---|---|
| Description | Représente le périphérique iDRAC de Dell. Le périphérique iDRAC doit être configuré comme dellRacDevice dans Active Directory. Cette configuration permet à iDRAC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory. |
| Type de classe | Classe structurelle |
| SuperClasses | dellProduct |
| Attributs | **dellSchemaVersion**<br>**dellRacType** |

**Tableau 7-4. 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**<br>**dellPrivilegeMember** |

**Tableau 7-5. Classe dellRAC4Privileges**

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

**Tableau 7-6. Classe dellPrivileges**

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

**Tableau 7-7. Classe dellProduct**

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

**Tableau 7-8. Liste des attributs ajoutés au schéma Active Directory**

| Nom / Description de l'attribut | OID attribué/Identifiant d'objet de syntaxe | Valeur unique |
|---|---|---|

| | | |
|---|---|---|
| **dellPrivilegeMember**<br><br>Liste des objets dellPrivilege qui appartiennent à cet attribut. | 1.2.840.113556.1.8000.1280.1.1.2.1<br><br>Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellProductMembers**<br><br>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.<br><br>Référence du lien : 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2<br><br>Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellIsLoginUser**<br><br>TRUE si l'utilisateur a les droits Ouvrir une session sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.3<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsCardConfigAdmin**<br><br>TRUE si l'utilisateur a les droits Configuration de carte sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.4<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsUserConfigAdmin**<br><br>TRUE si l'utilisateur a les droits Configuration utilisateur sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.5<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsLogClearAdmin**<br><br>TRUE si l'utilisateur a les droits Effacement de journal sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.6<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsServerResetUser**<br><br>TRUE si l'utilisateur a les droits Réinitialisation de serveur sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.7<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsConsoleRedirectUser**<br><br>TRUE si l'utilisateur a les droits Redirection de console sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.8<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsVirtualMediaUser**<br><br>TRUE si l'utilisateur a les droits Média virtuel sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.9<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsTestAlertUser**<br><br>TRUE si l'utilisateur a les droits Utilisateur pour l'alerte test sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.10<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsDebugCommandAdmin**<br><br>TRUE si l'utilisateur a les droits Administrateur pour la commande de débogage sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.11<br><br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellSchemaVersion**<br><br>La version de schéma actuelle est utilisée pour mettre à jour le schéma. | 1.2.840.113556.1.8000.1280.1.1.2.12<br><br>Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellRacType**<br><br>Cet attribut est le type de RAC actuel 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<br><br>Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellAssociationMembers**<br><br>Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut lié dellProductMembers.<br><br>Référence du lien : 12071 | 1.2.840.113556.1.8000.1280.1.1.2.14<br><br>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 Microsoft 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 iDRAC, les utilisateurs et les groupes d'utilisateurs, les associations iDRAC et les privilèges iDRAC.

Lorsque vous installez votre logiciel Systems Management Software à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez installer 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 Software. 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 Active Directory, consultez votre documentation Microsoft.

### Installation du pack administrateur

Vous devez installer le pack administrateur sur tous les systèmes qui gèrent les objets iDRAC d'Active Directory. Si vous n'installez pas le pack administrateur, vous ne pouvez pas afficher l'objet iDRAC Dell dans le conteneur.

Pour plus d'informations, consultez « Ouverture du snap-in Utilisateurs et ordinateurs Microsoft Active Directory ».

### Ouverture du snap-in Utilisateurs et ordinateurs Microsoft Active Directory

Pour ouvrir le snap-in Utilisateurs et ordinateurs Active Directory :

1. Si vous avez ouvert une session sur le 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, le pack administrateur Microsoft approprié doit être installé sur votre système local. Pour installer ce pack administrateur, cliquez sur **Démarrer**→ **Exécuter**, tapez `MMC` et appuyez sur **Entrée**.

   La MMC s'affiche.

2. Dans la fenêtre **Console 1**, cliquez sur **Fichier** (ou sur **Console** sur les systèmes exécutant Windows 2000).

3. Cliquez sur **Ajouter/Supprimer un snap-in**.

4. Sélectionnez le **Snap-in Utilisateurs et ordinateurs Active Directory** et cliquez sur **Ajouter**.

5. Cliquez sur **Fermer**, puis sur **OK**.

## Ajout d'utilisateurs iDRAC et de leurs privilèges à Microsoft Active Directory

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

- Créer un objet Périphérique iDRAC
- Créer un objet Privilège
- Créer un objet Association
- Configuration d'un objet Association

### Création d'un objet Périphérique iDRAC

1. Dans la fenêtre **Racine de la console** MMC, cliquez avec le bouton droit de la souris sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet avancé Gestion à distance Dell**.

   La fenêtre **Nouvel objet** s'affiche.

3. Tapez un nom pour le nouvel objet. Ce nom doit être identique au nom d'iDRAC que vous taperez à l'étape A de « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 ».

4. Sélectionnez **Objet Périphérique iDRAC**.

5. Cliquez sur **OK**.

### Création d'un objet Privilège

**REMARQUE :** Un objet Privilège doit être créé dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet avancé Gestion à distance Dell**.

   La fenêtre **Nouvel objet** s'affiche.

3. Tapez un nom pour le nouvel objet.

4. Sélectionnez **Objet Privilège**.
5. Cliquez sur **OK**.
6. Cliquez avec le bouton droit de la souris sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
7. Cliquez sur l'onglet **Privilèges de gestion à distance** et sélectionnez les privilèges que vous souhaitez donner à l'utilisateur.

## Création d'un objet Association

**REMARQUE :** L'objet Association iDRAC provient d'un groupe et sa portée est définie sur Domaine local.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau→ Objet avancé Gestion à distance Dell**.

   Cette action ouvre la fenêtre **Nouvel objet**.
3. Tapez un nom pour le nouvel objet.
4. Sélectionnez **Objet Association**.
5. Sélectionnez l'étendue de **l'objet Association**.
6. Cliquez sur **OK**.

## Configuration d'un objet Association

En utilisant la fenêtre **Propriétés de l'objet Association**, vous pouvez associer des utilisateurs, des groupes d'utilisateurs, des objets Privilège et des périphériques iDRAC.

Vous pouvez ajouter des groupes d'utilisateurs. La procédure de création de groupes associés à Dell et de groupes non associés à Dell est identique.

## Ajout d'utilisateurs ou de groupes d'utilisateurs

1. Cliquez avec le bouton droit de la souris sur **l'objet Association** et sélectionnez **Propriétés**.
2. Sélectionnez l'onglet **Utilisateurs** et cliquez sur **Ajouter**.
3. Tapez le nom de l'utilisateur ou du groupe d'utilisateurs et cliquez sur **OK**.

Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs durant l'authentification auprès d'un périphérique iDRAC. Vous ne pouvez ajouter qu'un seul objet Privilège à un objet Association.

## Ajout de privilèges

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Tapez le nom de l'objet Privilège et cliquez sur **OK**.

Cliquez sur l'onglet **Produits** pour ajouter un périphérique iDRAC connecté au réseau qui est disponible pour les utilisateurs ou groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques iDRAC à un objet Association.

## Ajout de périphériques iDRAC

Pour ajouter des périphériques iDRAC :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Tapez le nom du périphérique iDRAC et cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

## Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
4. Cliquez sur l'onglet **Réseau/Sécurité** → onglet **Service de répertoire**→ **Microsoft Active Directory**.
5. Allez à la fin de la page **Configuration et gestion d'Active Directory** et cliquez sur **Configurer Active Directory**.

   La page **Étape 1 sur 4 Configuration et gestion d'Active Directory** apparaît.
6. Sous **Paramètres du certificat**, cochez **Activer la validation de certificat** si vous voulez valider le certificat SSL de vos serveurs Active Directory ; sinon, passez à l'étape 9.
7. Sous **Téléverser le certificat AC d'Active Directory**, tapez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

   **REMARQUE :** Vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.
8. Cliquez sur **Téléverser**.

   Les informations concernant le certificat AC d'Active Directory que vous avez téléversé apparaissent.
9. Sous **Téléverser le fichier keytab Kerberos**, tapez le chemin du fichier keytab ou naviguez pour accéder au fichier. Cliquez sur **Téléverser**. Le fichier keytab Kerberos sera téléversé vers iDRAC6.
10. Cliquez sur **Suivant** pour passer à la page **Étape 2 sur 4 Configuration et gestion d'Active Directory**.
11. Cliquez sur **Activer Active Directory**.

**PRÉCAUTION : Dans cette version, les fonctionnalités Authentification bifactorielle (TFA) basée sur la carte à puce et Connexion directe (SSO) ne sont pas prises en charge si Active Directory est configuré pour le schéma étendu.**

12. Cliquez sur **Ajouter** pour saisir le nom de domaine utilisateur.
13. Tapez le nom de domaine utilisateur dans l'invite, puis cliquez sur **OK**. Notez que cette étape est facultative. Si vous configurez une liste de domaines utilisateur, la liste sera disponible dans l'écran d'ouverture de session de l'interface Web. Vous pouvez choisir dans la liste, puis vous devez seulement taper le nom d'utilisateur.
14. Tapez le **Délai d'expiration** en secondes pour spécifier le temps qu'iDRAC6 doit attendre avant d'obtenir une réponse d'Active Directory. La valeur par défaut est 120 secondes.
15. Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Les adresses 1 à 3 du serveur de contrôleur de domaine sont ignorées. Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Vous pouvez également sélectionner **Spécifier un domaine** et saisir le nom de domaine à utiliser dans le cadre de la recherche DNS. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Si **Schéma étendu** est sélectionné, les contrôleurs de domaine sont ceux où se trouvent l'objet Périphérique iDRAC6 et les objets Association.
16. Sélectionnez l'option **Spécifier les adresses du contrôleur de domaine** pour permettre à iDRAC6 d'utiliser les adresses du serveur de contrôleur de domaine Active Directory spécifiées. La recherche DNS n'est pas effectuée. Spécifiez l'adresse IP ou le nom de domaine pleinement qualifié (FQDN) des contrôleurs de domaine. Lorsque l'option **Spécifier les adresses du contrôleur de domaine** est sélectionnée, au moins l'une des trois adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si **Schéma étendu** est sélectionné, il s'agit des adresses des contrôleurs de domaine où se trouvent l'objet Périphérique iDRAC6 et les objets Association.

    **REMARQUE :** Le FQDN ou l'adresse IP que vous spécifiez dans le champ **Adresse du serveur de contrôleur de domaine** doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.
17. Cliquez sur **Suivant** pour passer à la page **Étape 3 sur 4 Configuration et gestion d'Active Directory**.
18. Sous **Sélection du schéma**, sélectionnez **Schéma étendu**.
19. Cliquez sur **Suivant** pour passer à la page **Étape 4 sur 4 Configuration et gestion d'Active Directory.**
20. Sous **Paramètres du schéma étendu**, tapez le nom d'iDRAC et son nom de domaine pour configurer l'objet Périphérique iDRAC. Le nom de domaine d'iDRAC est le domaine dans lequel l'objet iDRAC est créé.

21. Cliquez sur **Terminer** pour enregistrer les paramètres du schéma étendu d'Active Directory.

    Le serveur Web iDRAC6 vous renvoie automatiquement à la page **Configuration et gestion d'Active Directory**.

22. Cliquez sur **Paramètres de test** pour vérifier les paramètres du schéma étendu d'Active Directory.

23. Tapez votre nom d'utilisateur et votre mot de passe Active Directory.

    Les résultats du test et le journal du test sont affichés. Pour plus d'informations, consultez « Test de vos configurations ».

    **REMARQUE :** Vous devez posséder un serveur DNS correctement configuré sur iDRAC pour prendre en charge l'ouverture de session Active Directory. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**→ page **Réseau** pour configurer manuellement le(s) serveur(s) DNS ou utiliser DHCP pour obtenir le(s) serveur(s) DNS.

Vous avez terminé la configuration d'Active Directory avec le schéma étendu.

## Configuration de Microsoft Active Directory avec le schéma étendu avec la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Microsoft Active Directory iDRAC6 avec le schéma étendu à l'aide de l'outil CLI RACADM plutôt que 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 commun du RAC>

   racadm config -g cfgActiveDirectory -o cfgADRacDomain <nom de domaine rac pleinement qualifié>

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
   ```

   **REMARQUE :** Au moins l'une des 3 adresses doit être configurée. iDRAC tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Lorsque l'option Schéma étendu est sélectionnée, ces adresses sont les FQDN ou les adresses IP des contrôleurs de domaine où se trouve ce périphérique iDRAC. En mode schéma étendu, les serveurs de catalogue global ne sont pas du tout utilisés.

   **REMARQUE :** Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.

**PRÉCAUTION : Dans cette version, les fonctionnalités Authentification bifactorielle (TFA) basée sur la carte à puce et Connexion directe (SSO) ne sont pas prises en charge si Active Directory est configuré pour le schéma étendu.**

Pour désactiver la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

Dans ce cas, il n'est pas nécessaire de téléverser un certificat d'AC.

Pour faire appliquer la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

Dans ce cas, vous devez téléverser un certificat d'AC en utilisant la commande RACADM suivante :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

racadm sslcertupload -t 0x2 -f <certificat d'AC racine ADS>
```

L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, consultez « Importation du certificat SSL du micrologiciel iDRAC6 ».

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

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

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. Si DHCP est désactivé sur iDRAC ou que vous voulez entrer manuellement votre adresse 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 voulez configurer une liste de domaines utilisateur afin que vous ayez seulement besoin de saisir le nom d'utilisateur durant l'ouverture de session sur l'interface Web 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.

   Consultez « Utilisation de Microsoft Active Directory pour ouvrir une session sur iDRAC6 » pour plus de détails sur les domaines utilisateur.

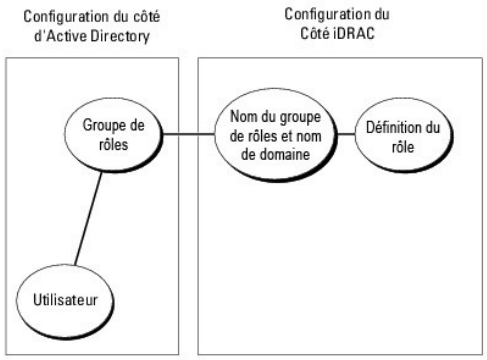
5. Appuyez sur **Entrée** pour terminer la configuration d'Active Directory avec le schéma étendu.

---

## Présentation d'Active Directory avec le schéma standard

Comme illustré dans la figure 7-3, l'utilisation du schéma standard pour l'intégration d'Active Directory nécessite une configuration sur Active Directory et sur iDRAC6.

**Figure 7-3. Configuration d'iDRAC avec Microsoft Active Directory et le schéma standard**




Du côté d'Active Directory, un objet 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 un iDRAC6 spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cet iDRAC6. Contrairement à la solution du schéma étendu, le rôle et le niveau de privilège sont définis sur chaque iDRAC6, et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque iDRAC. Le tableau 7-9 affiche les privilèges par défaut des groupes de rôles.

**Tableau 7-9. Privilèges par défaut des groupes de rôles**

| Groupes de rôles | Niveau de privilège par défaut | Droits accordés | Masque binaire |
|---|---|---|---|
| Groupe de rôles 1 | Administrateur | **Ouvrir une session sur iDRAC**, **Configurer iDRAC**, **Configurer des utilisateurs**, **Effacer des journaux**, **Exécuter des commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Alertes test**, **Exécuter des commandes de diagnostic** | 0x000001ff |
| Groupe de rôles 2 | Opérateur | **Ouvrir une session sur iDRAC**, **Configurer iDRAC**, **Exécuter des commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel, Alertes test, Exécuter des commandes de diagnosti**c | 0x000000f9 |
| Groupe de rôles 3 | Lecture seule | Ouvrir une session sur iDRAC | 0x00000001 |
| Groupe de rôles 4 | Aucun | Aucun droit attribué | 0x00000000 |
| Groupe de rôles 5 | Aucun | Aucun droit attribué | 0x00000000 |

**REMARQUE :** Les valeurs Masque binaire sont utilisées uniquement lors de la définition du schéma standard avec la RACADM.

## Scénario à domaine unique et scénario à plusieurs domaines

Si tous les utilisateurs d'ouverture de session et groupes de rôles ainsi que les groupes imbriqués se trouvent dans le même domaine, seules les adresses des contrôleurs de domaine doivent être configurées sur iDRAC6. Dans ce scénario à domaine unique, tous les types de groupe sont pris en charge.

Si tous les utilisateurs d'ouverture de session et groupes de rôles, ou l'un des groupes imbriqués, proviennent de domaines multiples, les adresses du serveur de catalogue global doivent être configurées sur iDRAC6. Dans ce scénario à plusieurs domaines, tous les groupes de rôles et groupes imbriqués, le cas échéant, doivent être du type Groupe universel.

## Configuration du schéma standard de Microsoft Active Directory pour accéder à iDRAC6

Vous devez effectuer les étapes suivantes pour configurer Active Directory pour qu'un utilisateur Active Directory puisse accéder 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 soit avec l'interface Web, soit avec la RACADM (consultez « Configuration de Microsoft Active Directory avec le schéma standard avec l'interface Web iDRAC6 » ou « Configuration de Microsoft Active Directory avec le schéma standard à l'aide de la RACADM »).
3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour avoir accès à iDRAC6.

## Configuration de Microsoft Active Directory avec le schéma standard avec l'interface Web iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
4. Cliquez sur l'onglet **Réseau/Sécurité** → onglet **Service de répertoire**→ **Microsoft Active Directory**.
5. Allez à la fin de la page **Configuration et gestion d'Active Directory** et cliquez sur **Configurer Active Directory**.

   La page **Étape 1 sur 4 Configuration et gestion d'Active Directory** apparaît.
6. Sous **Paramètres du certificat**, cochez **Activer la validation de certificat** si vous voulez valider le certificat SSL de vos serveurs Active Directory ; sinon, passez à l'étape 9**.**
7. Sous **Téléverser le certificat AC d'Active Directory**, tapez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

   **REMARQUE :** Vous devez tapez le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.
8. Cliquez sur **Téléverser**.

   Les informations concernant le certificat AC d'Active Directory valide s'affichent.
9. Sous **Téléverser le fichier eytab Kerberos**, tapez le chemin du fichier keytab ou naviguez pour accéder au fichier. Cliquez sur **Téléverser**. Le fichier keytab Kerberos est téléversé vers iDRAC6.
10. Cliquez sur **Suivant** pour passer à la page **Étape 2 sur 4 Configuration et gestion d'Active Directory**.
11. Sélectionnez **Activer Active Directory**.
12. Sélectionnez **Activer la connexion directe** si vous souhaitez ouvrir une session sur iDRAC6 sans saisir vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe.
13. Cliquez sur **Ajouter** pour saisir le nom de domaine utilisateur.
14. Tapez le nom de domaine utilisateur dans l'invite, puis cliquez sur **OK**.
15. Tapez le **Délai d'expiration** en secondes pour spécifier le temps qu'iDRAC6 doit attendre avant d'obtenir une réponse d'Active Directory. La valeur par défaut est 120 secondes.
16. Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Les adresses 1 à 3 du serveur de contrôleur de domaine sont ignorées. Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Vous pouvez également sélectionner **Spécifier un domaine** et saisir le nom de domaine à utiliser dans le cadre de la recherche DNS. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Si **Schéma standard** est sélectionné, les contrôleurs de domaine sont ceux où se trouvent les comptes d'utilisateur et les groupes de rôles.
17. Sélectionnez l'option **Spécifier les adresses du contrôleur de domaine** pour permettre à iDRAC6 d'utiliser les adresses du serveur de contrôleur de domaine Active Directory spécifiées. La recherche DNS n'est pas effectuée. Spécifiez l'adresse IP ou le nom de domaine pleinement qualifié (FQDN) des contrôleurs de domaine. Lorsque l'option **Spécifier les adresses du contrôleur de domaine** est sélectionnée, au moins l'une des trois adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si **Schéma standard** est sélectionné, il s'agit des adresses des contrôleurs de domaine où se trouvent les comptes d'utilisateur et les groupes de rôles.

**REMARQUE :** Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

18. Cliquez sur **Suivant** pour passer à la page **Étape 3 sur 4 Configuration et gestion d'Active Directory**.

19. Sous **Sélection du schéma**, sélectionnez **Schéma standard.**

20. Cliquez sur **Suivant** pour passer à la **page Étape 4a sur 4 Configuration et gestion d'Active Directory**.

21. Sélectionnez l'option **Rechercher les serveurs de catalogue global avec DNS** et saisissez le **nom de domaine racine** à utiliser dans le cadre d'une recherche DNS pour obtenir les serveurs de catalogue global Active Directory. Les adresses 1 à 3 du serveur de catalogue global sont ignorées. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Un serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.

22. Sélectionnez l'option **Spécifier les adresses du serveur de catalogue global** et saisissez l'adresse IP ou le nom de domaine pleinement qualifié (FQDN) du ou des serveur(s) de catalogue global. La recherche DNS n'est pas effectuée. Au moins l'une des trois adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Le serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.

    **REMARQUE :** Le FQDN ou l'adresse IP que vous spécifiez dans le champ **Adresse du serveur de catalogue global** doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.

    **REMARQUE :** Le serveur de catalogue global n'est requis que pour le schéma standard pour le cas où les comptes d'utilisateur et les groupes de rôles seraient dans des domaines différents. De plus, dans ce scénario à plusieurs domaines, seul le groupe universel peut être utilisé.

23. Sous **Groupes de rôles**, cliquez sur un **Groupe de rôles**.

    La page **Étape 4b sur 4 Configuration et gestion d'Active Directory s**'affiche.

24. Spécifiez le **Nom du groupe** de rôles.

    Le **Nom du groupe** de rôles identifie le groupe de rôles d'Active Directory associé à iDRAC.

25. Spécifiez le **Domaine du groupe** de rôles qui est le domaine du groupe de rôles.

26. Spécifiez les **Privilèges du groupe de rôles** en sélectionnant le **Niveau de privilège du groupe de rôles**. Par exemple, si vous sélectionnez **Administrateur**, tous les privilèges sont sélectionnés pour ce niveau de droit.

27. Cliquez sur **Appliquer** pour enregistrer les paramètres Groupe de rôles.

    Le serveur Web iDRAC6 vous renvoie automatiquement à la page **Étape 4a sur 4 Configuration et gestion d'Active Directory où vos paramètres sont affichés.**

28. Configurez des groupes de rôles supplémentaires, le cas échéant.

29. Cliquez sur **Terminer** pour revenir à la page **Configuration et gestion d'Active Directory**.

30. Cliquez sur **Paramètres de test** pour vérifier les paramètres du schéma standard d'Active Directory.

31. Tapez votre nom d'utilisateur et votre mot de passe iDRAC6.

    Les résultats du test et le journal du test sont affichés. Pour plus d'informations, consultez « Test de vos configurations ».

**REMARQUE :** Vous devez posséder un serveur DNS correctement configuré sur iDRAC pour prendre en charge l'ouverture de session Active Directory. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**→ page **Réseau** pour configurer manuellement le(s) serveur(s) DNS ou utiliser DHCP pour obtenir le(s) serveur(s) DNS.

Vous avez terminé la configuration d'Active Directory avec le schéma standard.

## Configuration de Microsoft Active Directory avec le schéma standard à l'aide de la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory iDRAC avec le schéma standard à l'aide de la CLI RACADM plutôt que 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 commun du groupe de rôles>
    ```

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupDomain <nom de domaine pleinement qualifié>

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Numéro de masque binaire pour
les droits utilisateur spécifiques>

**REMARQUE :** Pour les valeurs Numéro de masque binaire, consultez le tableau B-2.

racadm config -g cfgActiveDirectory -o cfgDomainController1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o cfgDomainController2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o cfgDomainController3 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

**REMARQUE :** Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

**REMARQUE :** Saisissez le FQDN du contrôleur de domaine, *et non* le FQDN du domaine uniquement. Par exemple, saisissez `servername.dell.com` au lieu de `dell.com`.

**REMARQUE :** Au moins une des 3 adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Avec le schéma standard, il s'agit des adresses des contrôleurs de domaine où les comptes d'utilisateur et les groupes de rôles sont situés.

racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

**REMARQUE :** Le serveur de catalogue global n'est requis que pour le schéma standard pour le cas où les comptes d'utilisateur et les groupes de rôles seraient dans des domaines différents. De plus, dans ce scénario à plusieurs domaines, seul le groupe universel peut être utilisé.

**REMARQUE :** Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

Pour désactiver la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0

Dans ce cas, aucun certificat d'autorité de certification (AC) ne doit être téléversé.

Pour faire appliquer la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

Dans ce cas, vous devez également téléverser le certificat d'AC en utilisant la commande RACADM suivante :

racadm sslcertupload -t 0x2 -f *<certificat d'AC racine ADS>*

L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, consultez « Importation du certificat SSL du micrologiciel iDRAC6 ».

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

2. Si DHCP est activé sur iDRAC6 et que vous voulez utiliser le DNS fourni par le serveur DHCP, tapez les commandes RACADM suivantes :

   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1

3. Si DHCP est désactivé sur iDRAC6 ou que vous voulez entrer manuellement votre adresse 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 voulez configurer une liste de domaines utilisateur afin que vous ayez seulement besoin de saisir le nom d'utilisateur durant l'ouverture de session sur l'interface Web, tapez la commande suivante :

   racadm config -g cfgUserDomain -o cfgUserDomainName -i <index>

   Jusqu'à 40 domaines utilisateur peuvent être configurés avec des numéros d'index compris entre 1 et 40.

   Consultez « Utilisation de Microsoft Active Directory pour ouvrir une session sur iDRAC6 » pour plus de détails sur les domaines utilisateur.

---

## Test de vos configurations

Pour vérifier si votre configuration fonctionne ou pour établir un diagnostic de l'échec de votre ouverture de session Active Directory, vous pouvez tester vos paramètres depuis l'interface Web iDRAC6.

Une fois la configuration des paramètres terminée dans l'interface Web iDRAC6, cliquez sur **Paramètres de test** au bas de la page. Il vous sera demandé de saisir un nom d'utilisateur de test (par exemple, nom d'utilisateur@domaine.com) et un mot de passe pour exécuter le test. Selon votre configuration, l'exécution de toutes les étapes du test et l'affichage des résultats de chaque étape peuvent prendre un certain temps. Un journal de test détaillé s'affichera au bas de la page de résultats.

En cas d'échec d'une étape, examinez les détails dans le journal de test pour identifier le problème et une éventuelle solution. Pour les erreurs les plus courantes, consultez « Questions les plus fréquentes concernant Active Directory ».

Si vous devez apporter des modifications à vos paramètres, cliquez sur l'onglet **Active Directory**, puis modifiez la configuration pas à pas.

---

## Activation de SSL sur un contrôleur de domaine

Lorsque iDRAC authentifie les utilisateurs par rapport à un contrôleur de domaine d'Active Directory, il démarre une session SSL avec le contrôleur de domaine. À ce stade, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (AC), dont le certificat racine est également téléversé vers iDRAC. En d'autres termes, pour qu'iDRAC soit capable de s'authentifier sur *n'importe quel* contrôleur de domaine, qu'il s'agisse du contrôleur de domaine racine ou enfant, ce contrôleur de domaine doit avoir un certificat activé SSL signé par l'AC du domaine.

Si vous utilisez l'AC 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 avec le bouton droit de la souris sur **Paramètres de requête automatique de certificat** et cliquez sur **Requête automatique de certificat**.
   c. Dans l'**Assistant Configuration de requêtes automatiques de certificats**, cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.
   d. Cliquez sur **Suivant**, puis sur **Terminer**.

## Exportation du certificat d'AC racine du contrôleur de domaine sur iDRAC6

**REMARQUE :** Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

**REMARQUE :** Si vous utilisez une AC autonome, les étapes suivantes peuvent varier.

1. Localisez le contrôleur de domaine qui exécute le service AC d'entreprise Microsoft.
2. Cliquez sur **Démarrer** → **Exécuter**.
3. Dans le champ **Exécuter**, tapez `mmc` et cliquez sur **OK**.
4. Dans la fenêtre **Console 1** (MMC), cliquez sur **Fichier (**ou **Console** pour les systèmes Windows 2000**)** et sélectionnez **Ajouter/Supprimer un snap- in**.
5. Dans la fenêtre **Ajouter/Supprimer un snap-in**, cliquez sur **Ajouter**.
6. Dans la fenêtre **Snap-in autonome**, sélectionnez **Certificats** et cliquez sur **Ajouter**.
7. Sélectionnez le **compte Ordinateur** et cliquez sur **Suivant**.
8. Sélectionnez **Ordinateur local** et cliquez sur **Terminer**.
9. Cliquez sur **OK**.
10. Dans la fenêtre **Console 1**, développez le dossier **Certificats**, puis le dossier **Personnel** et cliquez sur le dossier **Certificats**.
11. Repérez et cliquez avec le bouton droit de la souris sur le certificat d'AC racine, sélectionnez **Toutes les tâches** et cliquez sur **Exporter..**.
12. Dans l'**Assistant Exportation de certificat**, cliquez sur **Suivant** et sélectionnez **Ne pas exporter la clé privée**.
13. Cliquez sur **Suivant** et sélectionnez **Codé en base 64 X.509 (.cer)** comme format.
14. Cliquez sur **Suivant** et enregistrez le certificat dans un répertoire de votre système.
15. Téléversez le certificat que vous avez enregistré dans étape 14 vers iDRAC.

    Pour téléverser le certificat à l'aide de la RACADM, consultez « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 » ou « Configuration de Microsoft Active Directory avec le schéma standard à l'aide de la RACADM ».

Pour téléverser le certificat à l'aide de l'interface Web, consultez « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 » ou « Configuration de Microsoft Active Directory avec le schéma standard avec l'interface Web iDRAC6 ».

## Importation du certificat SSL du micrologiciel iDRAC6

**REMARQUE :** Si le serveur Active Directory est défini pour authentifier le client lors de la phase d'initialisation d'une session SSL, vous devez également téléverser le certificat du serveur iDRAC6 vers le contrôleur de domaine 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 de confiance de contrôleur de domaine.

**REMARQUE :** Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

**REMARQUE :** Si le certificat SSL du micrologiciel iDRAC6 est signé par une AC connue et si le certificat de cette AC est déjà dans la liste des autorités de certification racines de confiance du contrôleur de domaine, vous n'avez pas besoin d'effectuer les étapes décrites dans cette section.

Le certificat SSL iDRAC6 est le même que celui utilisé pour le serveur Web iDRAC6. Tous les contrôleurs iDRAC sont livrés avec un certificat auto-signé par défaut.

Pour télécharger le certificat SSL 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 avec le bouton droit de la souris sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
3. Cliquez sur **Suivant** et naviguez vers le fichier de certificat SSL.
4. Installez le certificat SSL iDRAC6 dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

   Si vous avez installé votre propre certificat, assurez-vous que l'AC 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 naviguez vers un magasin de votre choix.
6. Cliquez sur **Terminer,** puis sur **OK**.

---

## Utilisation de Microsoft Active Directory pour ouvrir une session sur iDRAC6

Vous pouvez utiliser Active Directory pour ouvrir une session sur iDRAC6 via une des méthodes suivantes :

- Interface Web
- RACADM distante
- Console série ou Telnet

La syntaxe d'ouverture de session est la même pour les trois méthodes :

*<nom d'utilisateur@domaine>*

ou

*<domaine>**<nom d'utilisateur>* ou *<domaine>*/*<nom d'utilisateur>*

où *nom d'utilisateur* est une chaîne ASCII de 1 à 256 octets.

Les espaces blancs et les caractères spéciaux (comme \, / ou @) ne peuvent pas être utilisés pour le nom d'utilisateur ou le nom de domaine.

**REMARQUE :** Vous ne pouvez pas spécifier de noms de domaine NetBIOS, tels que Amériques, car ces noms ne peuvent pas être résolus.

Si vous ouvrez une session depuis l'interface Web et que vous avez configuré des domaines utilisateur, la page d'ouverture de session de l'interface Web indiquera tous les domaines utilisateur parmi lesquels vous pouvez choisir dans le menu déroulant. Si vous sélectionnez un domaine utilisateur depuis le menu déroulant, il vous suffit de saisir le nom d'utilisateur. Si vous sélectionnez **Cet iDRAC**, vous pouvez toujours ouvrir une session en tant qu'utilisateur Active Directory en utilisant la syntaxe d'ouverture de session décrite ci-dessus dans « Utilisation de Microsoft Active Directory pour ouvrir une session sur iDRAC6 ».

Vous pouvez également ouvrir une session sur iDRAC6 à l'aide de la carte à puce. Pour plus d'informations, consultez « Ouverture de session sur iDRAC6 avec la carte à puce ».

**REMARQUE :** Le serveur Windows 2008 Active Directory prend uniquement en charge la chaîne <nom_d'utilisateur@<nom_de_domaine> avec 256 caractères maximum.

---

# Utilisation d'une connexion directe Microsoft Active Directory

Vous pouvez activer iDRAC6 pour utiliser Kerberos, un protocole d'authentification réseau, afin d'activer la connexion directe. Pour plus d'informations sur la configuration d'iDRAC6 pour utiliser la fonctionnalité Connexion directe d'Active Directory, consultez « Activation de l'authentification Kerberos ».

## Configuration d'iDRAC6 pour utiliser la connexion directe

1. Cliquez sur **Accès à distance**→ onglet **Réseau/Sécurité**→ onglet **Service de répertoire**→ **Microsoft Active Directory**→ et sélectionnez **Configurer Active Directory**.

2. Dans la page **Étape 2 sur 4 Configuration et gestion d'Active Directory**, sélectionnez **Activer la connexion directe**. L'option **Activer la connexion directe** est activée uniquement si vous avez sélectionné l'option **Activer Active Directory**.

   L'option **Activer la connexion directe** vous permet d'ouvrir une session sur iDRAC6 directement après avoir ouvert une session sur votre station de travail sans saisir vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Pour ouvrir une session sur iDRAC6 à l'aide de cette fonctionnalité, vous devez déjà être connecté à votre système via un compte d'utilisateur Active Directory valide. En outre, vous devez déjà avoir configuré le compte d'utilisateur pour ouvrir une session sur iDRAC6 à l'aide des références d'Active Directory. iDRAC6 utilise les références d'Active Directory mises en cache pour ouvrir une session.

   Pour activer la connexion directe à l'aide de la CLI, exécutez la commande racadm :

   ```
   racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
   ```

## Ouverture d'une session sur iDRAC6 à l'aide de la connexion directe

1. Ouvrez une session sur votre station de travail à l'aide de votre compte réseau.

2. Pour accéder à la page Web d'iDRAC6, tapez :

   https://<*adresse IP*>

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

   https://<*adresse IP*>:<*numéro de port*>

   où <*adresse IP*> est l'adresse IP d'iDRAC6 et *numéro de port* le numéro de port HTTPS.

   La page de connexion directe d'iDRAC6 s'affiche.

3. Cliquez sur **Ouvrir une session**.

iDRAC6 vous connecte à l'aide de vos références mises en cache dans le système d'exploitation lorsque vous avez ouvert une session avec votre compte Active Directory valide.

---

# Service de répertoire LDAP générique

iDRAC6 fournit une solution générique visant à prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne nécessite aucune extension de schéma au sein de vos services de répertoire.

Pour rendre l'implémentation LDAP iDRAC6 générique, les points communs entre les différents services de répertoire sont utilisés pour regrouper les utilisateurs, puis mapper la relation utilisateur-groupe. Le schéma constitue l'action spécifique au service de répertoire. Par exemple, ils peuvent avoir différents noms d'attribut pour le groupe, l'utilisateur et le lien entre l'utilisateur et le groupe. Ces actions peuvent être configurées dans iDRAC6.

## Syntaxe d'ouverture de session (utilisateur de répertoire et utilisateur local)

Contrairement à Active Directory, les caractères spéciaux (« @ », « \ » et « / ») ne sont pas utilisés pour différencier un utilisateur LDAP d'un utilisateur local. L'utilisateur d'ouverture de session doit uniquement saisir le nom d'utilisateur, à l'exclusion du nom de domaine. iDRAC6 adopte le nom d'utilisateur tel quel et ne le scinde pas en nom d'utilisateur et nom de domaine. Lorsque LDAP générique est activé, iDRAC6 tente d'abord de connecter l'utilisateur en tant qu'utilisateur de répertoire. En cas d'échec, la recherche d'utilisateur local est activée.

**REMARQUE :** Aucun changement de comportement n'a lieu au niveau de la syntaxe d'ouverture de session Active Directory. Lorsque LDAP générique est activé, la page d'ouverture de session d'IUG affiche uniquement « Cet iDRAC » dans le menu déroulant.

**REMARQUE :** Les caractères « < » et « > » ne sont pas autorisés dans le nom d'utilisateur pour les services de répertoire openLDAP et OpenDS.

## Configuration du service de répertoire LDAP générique avec l'interface Web iDRAC6

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

2. Ouvrez une session sur l'interface Web iDRAC6.

3. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.

4. Cliquez sur l'onglet **Réseau/Sécurité**→ onglet **Service de répertoire**→ **Service de répertoire LDAP générique**.

5. La page **Configuration et gestion de LDAP générique** affiche les paramètres LDAP générique iDRAC6 actuels. Faites défiler vers le bas de la page **Configuration et gestion de LDAP générique** et cliquez sur **Configurer LDAP générique**.

   **REMARQUE :** Dans cette version, seul le schéma standard Active Directory (SSAD) sans extension est pris en charge.

   La page **Étape 1 sur 3 Configuration et gestion de LDAP générique** apparaît. Utilisez cette page pour configurer le certificat numérique utilisé lors de l'établissement des connexions SSL au cours de la communication avec un serveur LDAP générique. Ces communications utilisent LDAP sur SSL (LDAPS). Si vous activez la validation de certificat, téléversez le certificat de l'autorité de certification (AC) qui a émis le certificat utilisé par le serveur LDAP lors de l'établissement des connexions SSL. Le certificat de l'AC est utilisé pour valider l'authenticité du certificat fourni par le serveur LDAP lors de l'établissement des connexions SSL.

   **REMARQUE :** Dans cette version, toute liaison LDAP basée sur un port autre que le port SSL n'est pas prise en charge. Seul LDAP sur SSL est pris en charge.

6. Sous **Paramètres du certificat**, cochez **Activer la validation de certificat** pour activer la validation de certificat. En cas d'activation, iDRAC6 utilise le certificat d'une AC pour valider le certificat du serveur LDAP lors de l'établissement de liaisons SSL (Secure Socket Layer) ; en cas de désactivation, iDRAC6 ignore l'étape de validation de certificat de l'établissement de liaisons SSL. Vous pouvez désactiver la validation de certificat au cours du test ou si votre administrateur système choisit de faire confiance aux contrôleurs de domaine dans l'étendue de sécurité sans valider leurs certificats SSL.

**PRÉCAUTION : Veillez à ce que CN = FQDN LDAP ouvert soit défini (par exemple, CN= openldap.lab) dans le champ Objet du certificat de serveur LDAP lors de la génération du certificat. Le champ Adresse du serveur LDAP d'iDRAC6 doit être défini pour correspondre à la même adresse FQDN afin que la validation de certificat puisse fonctionner.**

7. Sous **Téléverser le certificat AC du service de répertoire**, tapez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

   **REMARQUE :** Vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

8. Cliquez sur **Téléverser**.

   Le certificat de l'AC racine qui signe tous les certificats de serveur SSL (Security Socket Layer) des contrôleurs de domaine est téléversé.

9. Cliquez sur **Suivant** pour passer à la page **Étape 2 sur 3 Configuration et gestion de LDAP générique**. Utilisez cette page pour configurer les informations d'emplacement concernant les serveurs LDAP générique et les comptes d'utilisateur.

   **REMARQUE :** Dans cette version, les fonctionnalités Authentification bifactorielle (TFA) par carte à puce et Connexion directe (SSO) ne sont pas prises en charge dans le service de répertoire LDAP générique.

10. Sélectionnez **Activer LDAP générique**.

    **REMARQUE :** Dans cette version, le groupe imbriqué n'est pas pris en charge. Le micrologiciel recherche le membre direct du groupe pour le faire correspondre au nom unique d'utilisateur. En outre, seul le domaine unique est pris en charge. Le domaine croisé n'est pas pris en charge.

11. Cochez l'option **Utiliser le nom unique pour rechercher l'appartenance au groupe** pour utiliser le nom unique (DN) en tant que membres du groupe. iDRAC6 compare le nom unique d'utilisateur récupéré dans le répertoire aux membres du groupe. Si cette option est décochée, le nom d'utilisateur fourni par l'utilisateur d'ouverture de session est utilisé afin de le comparer aux membres du groupe.

12. Dans le champ **Adresse du serveur LDAP**, saisissez le nom de domaine pleinement qualifié (FQDN) ou l'adresse IP du serveur LDAP. Pour spécifier plusieurs serveurs LDAP redondants qui desservent le même domaine, fournissez la liste de tous les serveurs séparés par des virgules. iDRAC6 tente de se connecter à chaque serveur l'un après l'autre jusqu'à ce qu'une connexion soit établie.

13. Saisissez le port utilisé pour LDAP sur SSL dans le champ **Port du serveur LDAP**. Le port par défaut est 636.

14. Dans le champ **Nom unique de liaison**, saisissez le nom unique d'un utilisateur utilisé afin d'établir la liaison au serveur lors de la recherche du nom unique de l'utilisateur d'ouverture de session. S'il n'est pas spécifié, une liaison anonyme est utilisée.

15. Saisissez le **mot de passe de liaison** à utiliser en conjonction avec le **nom unique de liaison**. Ceci est obligatoire si la liaison anonyme n'est pas autorisée.

16. Dans le champ **Nom unique de base à rechercher**, saisissez le nom unique de la branche du répertoire à partir duquel toutes les recherches doivent débuter.

17. Dans le champ **Attribut de l'ouverture de session utilisateur**, saisissez l'attribut d'utilisateur à rechercher. L'attribut par défaut est UID. Il est recommandé de s'assurer de son unicité au sein du nom unique de base choisi, sinon un filtre de recherche doit être configuré afin de garantir l'unicité de l'utilisateur d'ouverture de session. Si le nom unique d'utilisateur ne peut pas être identifié de manière unique par la combinaison de recherche de l'attribut et du filtre de recherche, l'ouverture de session échoue.

18. Dans le champ **Attribut d'appartenance au groupe**, spécifiez quel attribut LDAP doit être utilisé pour rechercher l'appartenance au groupe. Il doit s'agir

d'un attribut de la classe de groupe. S'il n'est pas spécifié, iDRAC6 utilise les attributs *member* et *uniquemember*.

19. Dans le champ **Filtre de recherche**, saisissez un filtre de recherche LDAP valide. Utilisez le filtre si l'attribut d'utilisateur ne parvient pas à identifier de manière unique l'utilisateur d'ouverture de session dans le nom unique de base choisi. S'il n'est pas spécifié, la valeur est définie par défaut sur *objectClass=**, qui recherche tous les objets de l'arborescence. Ce filtre de recherche supplémentaire configuré par l'utilisateur s'applique uniquement à la recherche du nom unique d'utilisateur, et non à la recherche d'appartenance au groupe.

20. Cliquez sur **Suivant** pour passer à la page **Étape 3a sur 3 Configuration et gestion de LDAP générique**. Utilisez cette page pour configurer les groupes de privilèges utilisés pour autoriser les utilisateurs. Lorsque LDAP générique est activé, le ou les groupes de rôles sont utilisés pour spécifier la règle d'autorisation applicable aux utilisateurs iDRAC6.

    **REMARQUE :** Dans cette version, contrairement à AD, il n'est pas nécessaire d'avoir recours aux caractères spéciaux (« @ », « \ » et « / ») pour différencier un utilisateur LDAP d'un utilisateur local. Vous devez uniquement saisir votre nom d'utilisateur pour ouvrir une session et ne vous devez pas inclure le nom de domaine.

21. Sous **Groupes de rôles**, cliquez sur un **Groupe de rôles**.

    La page **Étape 3b sur 3 Configuration et gestion de LDAP générique a**pparaît. Utilisez cette page pour configurer chaque groupe de rôles utilisé pour contrôler la règle d'autorisation applicable aux utilisateurs.

22. Saisissez le **nom unique (DN) du groupe** qui identifie le groupe de rôles au sein du service de répertoire LDAP générique associé à iDRAC6.

23. Dans la section **Privilèges du groupe de rôles**, spécifiez les privilèges associés au groupe en sélectionnant le **niveau de privilège du groupe de rôles**. Par exemple, si vous sélectionnez **Administrateur**, tous les privilèges sont sélectionnés pour ce niveau de droit.

24. Cliquez sur **Appliquer** pour enregistrer les paramètres Groupe de rôles.

    Le serveur Web iDRAC6 vous renvoie automatiquement à la page **Étape 3a sur 3 Configuration et gestion de LDAP générique où vos paramètres Groupe de rôles sont affichés.**

25. Configurez des groupes de rôles supplémentaires, le cas échéant.

26. Cliquez sur **Terminer** pour revenir à la page récapitulative **Configuration et gestion de LDAP générique.**

27. Cliquez sur **Paramètres de test** pour vérifier les paramètres LDAP générique.

28. Saisissez le nom d'utilisateur et le mot de passe d'un utilisateur de répertoire choisi pour tester les paramètres LDAP. Le format dépend de l'*attribut d'ouverture de session utilisateur* utilisé et le nom d'utilisateur saisi doit correspondre à la valeur de l'attribut choisi.

    Les résultats du test et le journal du test sont affichés. Vous avez terminé la configuration du service de répertoire LDAP générique.

## Configuration du service de répertoire LDAP générique avec la RACADM

```
racadm config -g cfgldap -o cfgLdapEnable 1

racadm config -g cfgldap -o cfgLdapServer <FQDN ou adresse IP>

racadm config -g cfgldap -o cfgLdapPort <Numéro de port>

racadm config -g cfgldap -o cfgLdapBaseDN dc=common,dc=com

racadm config -g cfgldap -o cfgLdapCertValidationenable 0

racadm config -g cfgldaprolegroup -i 1 -o cfgLdapRoleGroupDN 'cn=everyone,ou=groups,dc=common,dc=com'

racadm config -g cfgldaprolegroup -i 1 -o cfgLdapRoleGroupPrivilege 0x0001
```

**Affichez les paramètres à l'aide des commandes ci-dessous**

```
racadm getconfig -g cfgldap

racadm getconfig -g cfgldaprolegroup -i 1
```

**Utilisez la RACADM pour confirmer si l'ouverture de session est possible**

```
racadm -r <iDRAC6-IP> -u user.1 -p password getractime
```

**Paramètres supplémentaires pour tester l'option Nom unique de liaison**

```
racadm config -g cfgldap -o cfgLdapBindDN "cn=idrac_admin,ou=iDRAC_admins,ou=People,dc=common,dc=com"

racadm config -g cfgldap -o cfgLdapBindPassword password
```

**REMARQUE :** Configurez iDRAC6 pour qu'il utilise un serveur de nom de domaine qui permettra de résoudre le nom d'hôte du serveur LDAP utilisé par iDRAC6 dans l'adresse de serveur LDAP. Le nom d'hôte doit correspondre au « CN » ou à l'« Objet » dans le certificat du serveur LDAP.

# Questions les plus fréquentes concernant Active Directory

**L'ouverture de session par SSO échoue sous Windows Server 2008 R2 x64. Que dois-je faire pour faire fonctionner SSO sous Windows Server 2008 R2 x64 ?**

1. Exécutez **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** pour le contrôleur de domaine et la règle de domaine. Configurez vos ordinateurs pour qu'ils utilisent la suite de cryptage DES-CBC-MD5. Ces paramètres peuvent avoir une incidence sur la compatibilité avec les ordinateurs ou services clients et les applications de votre environnement. Le paramètre de règle **Configurer les types de cryptage autorisés pour Kerberos** se trouve sous **Configuration ordinateur\Paramètres de sécurité\Règles locales\Options de sécurité**.

2. Les clients de domaine doivent disposer du GPO à jour. À la ligne de commande, tapez `gpupdate /force` et supprimez l'ancien fichier keytab grâce à la commande `klist purge`.

3. Une fois le GPO mis à jour, créez le nouveau fichier keytab.

4. Téléversez le fichier keytab vers iDRAC6.

SSO fonctionne désormais avec iDRAC6.

**Mon ouverture de session Active Directory a échoué. Comment puis-je résoudre le problème ?**

iDRAC6 offre un outil de diagnostic dans l'interface Web. Ouvrez une session en tant qu'utilisateur local avec des droits Administrateur depuis l'interface Web. Cliquez sur **Accès à distance**→ onglet **Réseau/Sécurité**→ **Service de répertoire**→ **Microsoft Active Directory**. Allez à la fin de la page **Configuration et gestion d'Active Directory** et cliquez sur **Paramètres de test**. Saisissez un nom d'utilisateur et un mot de passe de test, puis cliquez sur **Démarrer le test**. iDRAC6 lance les tests étape par étape et affiche les résultats de chaque étape. Un résultat de test détaillé est également journalisé pour vous aider à résoudre tout problème. Retournez à la page **Configuration et gestion d'Active Directory**. Allez à la fin de la page et cliquez sur **Configurer Active Directory** pour modifier votre configuration et exécuter de nouveau le test jusqu'à ce que l'utilisateur du test réussisse l'étape d'authentification.

**J'ai activé la validation de certificat, mais mon ouverture de session Active Directory a échoué. J'ai exécuté les diagnostics depuis l'IUG et les résultats du test affichent le message d'erreur suivant :ERREUR : impossible de contacter le serveur LDAP, erreur : 14090086:routines SSL :SSL3_GET_SERVER_CERTIFICATE : échec de la vérification du certificat : veuillez vérifier que le certificat de l'AC correct a été téléversé vers iDRAC. Veuillez également vérifier que la date d'iDRAC est comprise dans la période de validité des certificats et que l'adresse du contrôleur de domaine configurée dans iDRAC correspond à l'objet du certificat de serveur de répertoire**.

**Quel peut être le problème et comment le résoudre ?**

Si la validation de certificat est activée, iDRAC6 utilise le certificat d'AC téléversé pour vérifier le certificat du serveur de répertoire lorsqu'iDRAC6 établit la connexion SSL avec le serveur de répertoire. Les raisons les plus courantes de l'échec de la validation de certificat sont :

1. La date d'iDRAC6 n'est pas comprise dans la période de validité du certificat de serveur ou du certificat d'AC. Vérifiez l'heure d'iDRAC6 et la période de validité de votre certificat.

2. Les adresses du contrôleur de domaine configurées dans iDRAC6 ne correspondent pas à l'objet ou à l'autre nom de l'objet du certificat de serveur de répertoire. Si vous utilisez une adresse IP, veuillez lire la question et la réponse suivantes. Si vous utilisez un FQDN, veuillez vous assurer que vous utilisez le FQDN du contrôleur de domaine, et non le domaine, par exemple, `nomduserveur.exemple.com` au lieu de `exemple.com`.

**J'utilise une adresse IP comme adresse de contrôleur de domaine et je ne suis pas parvenu à valider le certificat. Quel est le problème ?**

Cochez le champ Objet ou Autre nom de l'objet du certificat de votre contrôleur de domaine. Active Directory utilise généralement le nom d'hôte, et non l'adresse IP, du contrôleur de domaine dans le champ Objet ou Autre nom de l'objet du certificat du contrôleur de domaine. Vous pouvez résoudre le problème de plusieurs façons :

1. Configurer le nom d'hôte (FQDN) du contrôleur de domaine en tant qu'*adresse(s) du contrôleur de domaine* sur iDRAC6 afin de correspondre à l'objet ou à l'autre nom de l'objet du certificat de serveur.

2. Émettre à nouveau le certificat de serveur pour utiliser une adresse IP dans le champ Objet ou Autre nom de l'objet afin que celui-ci corresponde à l'adresse IP configurée dans iDRAC6.

3. Désactiver la validation de certificats si vous choisissez de faire confiance à ce contrôleur de domaine sans validation de certificat durant l'établissement de liaisons SSL.

J'utilise un schéma étendu dans un environnement à domaines multiples. Comment dois-je configurer les adresses du contrôleur de domaine ?

Utilisez le nom d'hôte (FQDN) ou l'adresse IP du ou des contrôleurs de domaine desservant le domaine dans lequel l'objet iDRAC6 réside.

Dois-je configurer la ou les adresses du catalogue global ?

Si vous utilisez un schéma étendu, l'adresse du catalogue global n'est pas utilisée.

Si vous utilisez le schéma standard et que les utilisateurs et les groupes de rôles proviennent de domaines différents, une ou des adresses du catalogue global sont requises. Dans ce cas, seul le groupe universel peut être utilisé.

Si vous utilisez le schéma standard et que tous les utilisateurs et groupes de rôles proviennent du même domaine, une ou des adresses du catalogue global ne sont pas requises.

Comment fonctionne la requête de schéma standard ?

iDRAC6 se connecte tout d'abord à ou aux adresses du contrôleur de domaine configurées et si l'utilisateur et les groupes de rôles sont dans ce domaine, les privilèges seront enregistrés.

Si une ou des adresses de contrôleur global sont configurées, iDRAC6 continue d'interroger le catalogue global. Si des privilèges supplémentaires sont récupérés du catalogue global, ces privilèges sont accumulés.

iDRAC6 utilise-t-il toujours LDAP sur SSL ?

Oui. Tous les transports se font via le port sécurisé 636 et/ou 3269.

Durant la *définition du test*, iDRAC6 effectue une connexion LDAP CONNECT uniquement pour aider à isoler le problème, mais il n'effectue pas de liaison LDAP BIND sur une connexion non sécurisée.

Pourquoi iDRAC6 active-t-il la validation de certificat par défaut ?

iDRAC6 renforce la sécurité afin d'assurer l'identité du contrôleur de domaine auquel iDRAC6 se connecte. À défaut de la validation de certificat, un pirate pourrait usurper un contrôleur de domaine et détourner la connexion SSL. Si vous choisissez de faire confiance à tous les contrôleurs de domaine de votre étendue de sécurité sans validation de certificat, vous pouvez la désactiver via l'IUG ou la CLI.

iDRAC6 prend-il en charge le nom NetBIOS ?

Pas dans cette version.

**Que dois-je vérifier si je ne parviens pas à ouvrir une session sur iDRAC6 avec Active Directory ?**

Vous pouvez diagnostiquer le problème en cliquant sur **Paramètres de test** au bas de la page **Configuration et gestion d'Active Directory** dans l'interface Web iDRAC6. Corrigez ensuite le problème spécifique indiqué par les résultats du test. Pour plus d'informations, consultez « Test de vos configurations ».

**La plupart des problèmes courants sont expliqués dans cette section ; toutefois, en général, vous devez 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 sur iDRAC6 à l'aide de vos références locales.

   Lorsque vous avez ouvert une session :

   a. Vérifiez que vous avez coché l'option **Activer Active Directory** dans la page **Configuration et gestion d'Active Directory** iDRAC6.

   b. Vérifiez que le paramètre DNS est correct sur la page Configuration de la mise en réseau iDRAC6.

   c. Assurez-vous que vous avez téléversé le bon certificat ACracine d'Active Directory vers iDRAC6 si vous avez activé la validation de certificat. Assurez-vous que l'heure d'iDRAC6 est comprise dans la période de validité du certificat AC.

   d. Si vous utilisez le schéma étendu, assurez-vous que le **nom d'i**DRAC6 et le **nom de domaine i**DRAC6 correspondent à la configuration de votre environnement Active Directory.

      Si vous utilisez le schéma standard, assurez-vous que le **nom du groupe** et le **nom de domaine du groupe** correspondent à votre configuration Active Directory.

3. Vérifiez les certificats SSL du contrôleur de domaine pour vous assurer que l'heure iDRAC6 est comprise dans la période de validité du certificat.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Configuration de l'authentification par carte à puce

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



iDRAC6 prend en charge la fonctionnalité Authentification bifactorielle (TFA) en activant **l'ouverture de session par carte à puce**.

Les schémas d'authentification standard utilisent le nom d'utilisateur et le mot de passe pour authentifier les utilisateurs. Ils n'offrent qu'une sécurité minimale.

Pour sa part, la TFA offre un niveau accru de sécurité en exigeant que les utilisateurs fournissent deux facteurs d'authentification : ce qu'ils ont (la carte à puce, un périphérique physique) et ce qu'ils savent (un code secret tel qu'un mot de passe ou un code PIN).

L'authentification bifactorielle exige des utilisateurs qu'ils vérifient leur identité en fournissant *les deux* facteurs.

---

## Configuration de l'ouverture de session par carte à puce sur iDRAC6

Pour activer la fonctionnalité Ouverture de session par carte à puce iDRAC6 à partir de l'interface Web, accédez à **Accès à distance**→ **Réseau/Sécurité**→ **Carte à puce et sélectionnez Activer**.

Si vous sélectionnez :

- **Activer** ou **Activer avec la racadm distante**, vous êtes invité à ouvrir une session par carte à puce au cours des tentatives d'ouverture de session ultérieures avec l'interface Web.

  Lorsque vous sélectionnez **Activer**, toutes les interfaces hors bande de l'interface de ligne de commande (CLI), telles que Telnet, SSH, série, RACADM distante et IPMI sur LAN, sont désactivées, car ces services prennent en charge uniquement l'authentification monofactorielle.

  Lorsque vous sélectionnez **Activer avec la racadm distante**, toutes les interfaces hors bande de la CLI, à l'exception de la RACADM distante, sont désactivées.

  **REMARQUE :** Il est recommandé que l'administrateur d'iDRAC6 utilise le paramètre **Activer avec la racadm distante** uniquement pour accéder à l'interface Web iDRAC6 afin d'exécuter des scripts à l'aide des commandes de la RACADM distante. Si l'administrateur n'a pas besoin d'utiliser la RACADM distante, il est recommandé d'utiliser le paramètre **Activé** pour l'ouverture de session par carte à puce. Assurez-vous que la configuration des utilisateurs locaux d'iDRAC6 et/ou la configuration d'Active Directory a été achevée avant d'activer la fonctionnalité **Ouverture de session par carte à puce**.

- **Désactivez** la configuration de la carte à puce (par défaut). Cette sélection désactive la fonctionnalité Ouverture de session par carte à puce TFA et à la prochaine ouverture de session sur l'IUG d'iDRAC6, vous êtes invité à saisir un nom d'utilisateur et un mot de passe d'ouverture de session Microsoft® Active Directory® ou local, qui se présente sous la forme d'une invite d'ouverture de session par défaut de l'interface Web.
- **Activez le contrôle CRL pour l'ouverture de session par carte à puce**. Le certificat iDRAC de l'utilisateur, qui est téléchargé depuis le serveur de distribution de la liste de révocation de certificat (LRC), est contrôlé pour vérifier sa révocation dans la LRC.

  **REMARQUE :** Les serveurs de distribution LRC sont répertoriés dans les certificats de la carte à puce des utilisateurs.

---

## Configuration des utilisateurs d'iDRAC6 local pour l'ouverture de session par carte à puce

Vous pouvez configurer les utilisateurs d'iDRAC6 local pour qu'ils ouvrent une session sur iDRAC6 au moyen de la carte à puce. Cliquez sur **Accès à distance**→ **Réseau/Sécurité**→ **Utilisateurs**.

Toutefois, pour que l'utilisateur puisse ouvrir une session sur iDRAC6 avec la carte à puce, vous devez téléverser le certificat de la carte à puce de l'utilisateur et le certificat de l'autorité de certification (AC) de confiance vers iDRAC6.

### Exportation du certificat de la carte à puce

Vous pouvez obtenir le certificat de l'utilisateur en exportant le certificat de la carte à puce à l'aide du logiciel de gestion de carte (CMS) de la carte à puce vers un fichier sous le format encodé Base64. Vous pouvez généralement obtenir le CMS auprès du fournisseur de la carte à puce. Ce fichier encodé doit être téléversé en tant que certificat de l'utilisateur vers iDRAC6. L'autorité de certification de confiance qui émet les certificats de l'utilisateur de carte à puce doit également exporter le certificat d'une AC vers un fichier au format encodé Base64. Vous devez téléverser ce fichier en tant que certificat d'une AC de confiance pour l'utilisateur. Configurez l'utilisateur avec le nom d'utilisateur qui forme le nom de principe d'utilisateur (UPN) de l'utilisateur dans le certificat de la carte à puce.

**REMARQUE :** Pour ouvrir une session sur iDRAC6, le nom d'utilisateur que vous configurez dans iDRAC6 doit avoir la même casse que le nom de principe d'utilisateur (UPN) dans le certificat de la carte à puce.

Par exemple, si le certificat de la carte à puce a été émis pour l'utilisateur, « exempleutilisateur@domaine.com », le nom d'utilisateur doit être configuré comme « exempleutilisateur ».

---

## Configuration des utilisateurs d'Active Directory pour l'ouverture de session par carte à puce

Pour configurer les utilisateurs d'Active Directory pour qu'ils ouvrent une session sur iDRAC6 au moyen de la carte à puce, l'administrateur d'iDRAC6 doit configurer le serveur DNS, téléverser le certificat AC Active Directory sur iDRAC6 et activer l'ouverture de session Active Directory. Consultez « Utilisation du service de répertoire iDRAC6 » pour plus d'informations sur la configuration des utilisateurs d'Active Directory.

**REMARQUE :** Si l'utilisateur de la carte à puce figure dans Active Directory, un mot de passe Active Directory est exigé ainsi que le code PIN de la carte à puce.

Vous pouvez configurer Active Directory depuis **Accès à distance→ Réseau/Sécurité→ Service de répertoire→Microsoft Active Directory.**

---

## Configuration de la carte à puce

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

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Carte à puce**.
3. Configurez les paramètres Ouverture de session par carte à puce.

   Le tableau 8-1 fournit des informations sur les paramètres de la page **Carte à puce**.
4. Cliquez sur **Appliquer**.

**Tableau 8-1. Paramètres de la carte à puce**

| Paramètre | Description |
|---|---|
| **Configurer l'ouverture de session par carte à puce** | • **Désactivé :** désactive l'ouverture de session par carte à puce. Les ouvertures de session ultérieures depuis l'interface utilisateur graphique (IUG) affichent la page d'ouverture de session habituelle. Toutes les interfaces hors bande de la ligne de commande, y compris Secure Shell (SSH), Telnet, série et la RACADM distante, sont définies sur leur état par défaut.<br>• **Activé :** active l'ouverture de session par carte à puce. Après avoir appliqué les modifications, fermez la session, insérez votre carte à puce, puis cliquez sur **Ouvrir une session** pour saisir le code PIN de votre carte à puce. L'activation de l'ouverture de session par carte à puce désactive toutes les interfaces hors bande de la CLI, y compris SSH, Telnet, série, la RACADM distante et IPMI sur LAN.<br>• **Activé avec la racadm distante :** active l'ouverture de session par carte à puce en même temps que la RACADM distante. Toutes les autres interfaces hors bande de la CLI sont désactivées.<br><br>**REMARQUE :** L'ouverture de session par carte à puce vous impose de configurer les utilisateurs d'iDRAC6 local avec les certificats appropriés. Si l'ouverture de session par carte à puce sert à ouvrir une session pour un utilisateur Microsoft Active Directory, vous devez vous assurer que vous avez bien configuré le certificat d'utilisateur Active Directory pour cet utilisateur. Vous pouvez configurer le certificat d'utilisateur dans la page **Utilisateurs→ Menu principal utilisateurs**. |
| **Activer le contrôle CRL pour l'ouverture de session par carte à puce** | Ce contrôle est disponible uniquement pour les utilisateurs locaux de la carte à puce. Sélectionnez cette option si vous souhaitez qu'iDRAC6 contrôle la liste de révocation de certificat (CRL) pour vérifier si le certificat de la carte à puce de l'utilisateur a été révoqué. Pour que la fonctionnalité CRL puisse fonctionner, une adresse IP DNS valide doit être configurée sur iDRAC6 dans sa configuration réseau. Vous pouvez configurer l'adresse IP DNS dans iDRAC6 sous **Accès à distance→ Réseau/Sécurité→ Réseau**.<br><br>L'utilisateur ne sera pas en mesure d'ouvrir une session si :<br><br>• Le certificat d'utilisateur est répertorié comme révoqué dans le fichier CRL.<br>• iDRAC6 n'est pas en mesure de communiquer avec le serveur de distribution CRL.<br>• iDRAC6 n'est pas en mesure de télécharger la CRL.<br><br>**REMARQUE :** Vous devez configurer correctement l'adresse IP du serveur DNS dans la page **Réseau/Sécurité→ Réseau** pour que ce contrôle réussisse. |

---

## Ouverture de session sur iDRAC6 avec la carte à puce

L'interface Web d'iDRAC6 affiche la page Ouverture de session par carte à puce pour tous les utilisateurs qui sont configurés pour utiliser la carte à puce.

**REMARQUE :** Assurez-vous que la configuration des utilisateurs locaux d'iDRAC6 et/ou la configuration d'Active Directory a été achevée avant d'activer l'ouverture de session par carte à puce pour l'utilisateur.

**REMARQUE :** Selon les paramètres de votre navigateur, il se peut que vous soyez invité à télécharger et à installer le plug-in ActiveX du lecteur de carte à puce lorsque vous utilisez cette fonctionnalité pour la première fois.

1. Accédez à la page Web d'iDRAC6 avec https.

   https://<*adresse IP*>

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

   https://<*adresse IP*>:<*numéro de port*>

   où <*adresse IP*> est l'adresse IP d'iDRAC6 et *numéro de port* le numéro de port HTTPS.

   La page Ouverture de session iDRAC6 apparaît et vous invite à insérer la carte à puce.

2. Insérez la carte à puce dans le lecteur et cliquez sur **Ouvrir une session**.

   iDRAC6 vous invite à saisir le code PIN de la carte à puce.

3. Saisissez le code PIN de la carte à puce pour les utilisateurs locaux de la carte à puce et si l'utilisateur n'est pas créé localement, iDRAC6 vous invite à saisir le mot de passe pour le compte Active Directory de l'utilisateur.

**REMARQUE :** Si vous êtes un utilisateur d'Active Directory pour lequel **Activer le contrôle CRL pour l'ouverture de session par carte à puce** est sélectionné, iDRAC6 tente de télécharger la CRL et contrôle celle-ci pour le certificat de l'utilisateur. L'ouverture de session via Active Directory échoue si le certificat est répertorié comme révoqué dans la CRL ou si la CRL ne peut pas être téléchargée pour une raison quelconque.

Vous avez ouvert une session sur iDRAC6.

---

## Ouverture d'une session sur iDRAC6 avec l'authentification par carte à puce Active Directory

1. Ouvrez une session sur iDRAC6 avec https.

   https://<*adresse IP*>

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

   https://<*adresse IP*>:<*numéro de port*>

   où <*adresse IP*> est l'adresse IP d'iDRAC6 et *numéro de port* le numéro de port HTTPS.

   La page Ouverture de session iDRAC6 apparaît et vous invite à insérer la carte à puce.

2. Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.

   La boîte de dialogue contextuelle Code PIN s'affiche.

3. Saisissez le code PIN, puis cliquez sur **OK**.

4. Saisissez le mot de passe Active Directory de l'utilisateur pour authentifier l'utilisateur et cliquez sur **OK**.

   Vous avez ouvert une session sur iDRAC6 avec vos références telles qu'elles sont définies dans Active Directory.

**REMARQUE :** Si l'utilisateur de la carte à puce est présent dans Active Directory, un mot de passe Active Directory est exigé ainsi que le code PIN de la carte à puce. Dans les versions ultérieures, le mot de passe Active Directory peut ne pas être requis.

---

## Dépannage de l'ouverture de session par carte à puce dans iDRAC6

Utilisez les astuces suivantes pour déboguer une carte à puce inaccessible :

### Plug-in ActiveX incapable de détecter le lecteur de cartes à puce

Vérifiez que la carte à puce est bien prise en charge sur le système d'exploitation Microsoft Windows®. Windows prend en charge un nombre limité de fournisseurs de services cryptographiques (CSP) de cartes à puce.

Astuce : en règle générale, pour vérifier si les CSP de carte à puce sont présents sur un client donné, insérez la carte à puce dans le lecteur lorsque l'écran d'ouverture de session de Windows apparaît (Ctrl-Alt-Suppr) et vérifiez si Windows détecte bien la carte à puce et affiche la boîte de dialogue Code NIP.

## Code NIP de la carte à puce incorrect

Vérifiez si la carte à puce a été bloquée suite à un nombre trop élevé de tentatives avec un code PIN incorrect. Dans ces cas, l'émetteur de la carte à puce dans l'organisation peut vous aider à obtenir une nouvelle carte à puce.

## Impossible d'ouvrir une session sur l'iDRAC6 local

Si un utilisateur d'iDRAC6 local ne parvient pas à ouvrir une session, vérifiez si le nom d'utilisateur et les certificats d'utilisateur téléversés sur iDRAC6 ont expiré. Les journaux de suivi d'iDRAC6 peuvent fournir des messages de journal importants sur les erreurs, bien que les messages d'erreur soient parfois intentionnellement ambigus pour des raisons de sécurité.

## Impossible d'ouvrir une session sur iDRAC6 en tant qu'utilisateur d'Active Directory

- Si vous ne parvenez pas à ouvrir une session sur iDRAC6 en tant qu'utilisateur d'Active Directory, essayez d'ouvrir une session sur iDRAC6 sans activer l'ouverture de session par carte à puce. Si vous avez activé le contrôle CRL, essayez d'ouvrir une session sur Active Directory sans activer le contrôle CRL. Le journal de suivi d'iDRAC6 doit fournir des messages importants en cas de défaillance de la CRL.
- Vous avez également la possibilité de désactiver l'ouverture de session par carte à puce via la racadm locale à l'aide de la commande suivante : `racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0`
- Pour les plateformes Windows 64 bits, le plug-in Active-X d'authentification iDRAC6 ne s'installera pas correctement si une version 64 bits du « progiciel redistribuable Microsoft Visual C++ 2005 » est déployée. Pour installer et exécuter le plug-in Active-X correctement, déployez la version 32 bits du « progiciel redistribuable Microsoft Visual C++ 2005 SP1 (x86) ». Ce progiciel est requis pour lancer la session vKVM sur un navigateur Internet Explorer.
- Si vous obtenez le message d'erreur suivant « Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in » (Impossible de charger le plug-in de carte à puce. Vérifiez vos paramètres IE. Il se peut également que vous ne disposiez pas de privilèges suffisants pour pouvoir utiliser le plug-in de carte à puce), installez alors le « progiciel redistribuable Microsoft Visual C++ 2005 SP1 (x86) ». Ce fichier est disponible sur le site Web de Microsoft à l'adresse **www.microsoft.com**. Deux versions distribuées du progiciel redistribuable C++ ont été testées et permettent le chargement du plug-in de carte à puce Dell. Pour plus d'informations, consultez le tableau 8-2.

**Tableau 8-2. Versions distribuées du progiciel redistribuable C++**

| Nom du fichier du progiciel redistribuable | Version | Date de diffusion | Taille | Description |
|---|---|---|---|---|
| vcredist_x86.exe | 6.0.2900.2180 | 21 mars 2006 | 2,56 Mo | MS Redistributable 2005 |
| vcredist_x86.exe | 9.0.21022.8 | 7 novembre 2007 | 1,73 Mo | MS Redistributable 2008 |

- Vérifiez que la différence entre l'heure d'iDRAC6 et l'heure du contrôleur de domaine sur le serveur du contrôleur de domaine est de 5 minutes au plus afin que l'authentification Kerberos puisse fonctionner. Vérifiez l'**Heure du RAC** sur la page **Système→ Accès à distance→ Propriétés→ Informations sur iDRAC** et l'heure du contrôleur de domaine en cliquant avec le bouton droit de la souris sur l'heure dans le coin inférieur droit de l'écran. Le décalage de fuseau horaire est affiché dans l'affichage contextuel. Pour l'heure normale du centre des États-Unis (CST), ce décalage est de - 6). Utilisez la commande de décalage du fuseau horaire RACADM suivante pour synchroniser l'heure d'iDRAC6 (via la RACADM distante ou Telnet/SSH) : `racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <valeur du décalage en minutes>`. Par exemple, si l'heure système est GMT -6 (heure normale du centre des États-Unis) et que l'heure est 14h00, définissez l'heure d'iDRAC6 sur 18h00 GMT, ce qui vous oblige à saisir « 360 » dans la commande ci-dessus pour le décalage. Vous pouvez également utiliser *cfgRacTuneDaylightoffset* afin de prendre en compte la variation de l'heure d'été. Vous n'aurez ainsi plus à changer l'heure à ces deux périodes de l'année où les ajustements d'heures sont effectués ou prenez-les tout simplement en compte dans le décalage ci-dessus en saisissant « 300 » dans l'exemple ci-dessus.

---

Retour à la page du sommaire

Retour à la page du sommaire

# Utilisation de la redirection de console d'IUG

**Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.3**



Cette section fournit des informations sur l'utilisation de la fonctionnalité Redirection de la console iDRAC6.

---

## Présentation

La fonctionnalité Redirection de console iDRAC6 vous permet d'accéder à la console locale à distance en mode graphique ou texte. À l'aide de la redirection de la console, vous pouvez contrôler un ou plusieurs systèmes activés iDRAC6 à partir d'un seul emplacement.

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

---

## Utilisation de la redirection de console

**REMARQUE :** Quand vous ouvrez une session de redirection de console, le serveur géré n'indique pas que la console a été redirigée.

**REMARQUE :** Si une session de redirection de console est déjà ouverte depuis la station de gestion vers iDRAC6, une tentative pour ouvrir une nouvelle session à partir de la station de gestion vers cet iDRAC6 entraîne l'activation de la session existante. Une nouvelle session n'est pas générée.

**REMARQUE :** Il est possible d'ouvrir simultanément des sessions de redirection de console multiples à partir d'une station de gestion unique vers plusieurs contrôleurs iDRAC6.

La page **Redirection de la 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 :

- Quatre sessions de redirection de console simultanées sont prises en charge au maximum. Toutes les sessions affichent la même console de serveur géré simultanément.
- Deux sessions peuvent être ouvertes vers un serveur distant (une par type de plug-in) à partir de la même console client (station de gestion). Il est possible d'ouvrir sur le même client des sessions multiples vers plusieurs serveurs distants.
- Une session de redirection de console ne doit pas être lancée à partir d'un navigateur Web sur le système géré.
- Une bande passante réseau disponible minimale de 1 Mo/s est exigée.

La première session de redirection de console vers iDRAC6 est une session à accès complet. Si un deuxième utilisateur effectue une demande de session de redirection de console, le premier utilisateur est averti et la possibilité lui est offerte d'envoyer une requête de partage au deuxième utilisateur. Le deuxième utilisateur est averti qu'un autre utilisateur contrôle la session.

### Configuration de votre station de gestion

Pour utiliser la redirection de console sur votre station de gestion, procédez comme suit :

1. Installez et configurez un navigateur Web pris en charge. Consultez les sections suivantes pour plus d'informations :
   - « Navigateurs Web pris en charge »
   - « Configuration d'un navigateur Web pris en charge »
2. Si vous utilisez Firefox ou souhaitez utiliser le visualiseur Java® avec Internet Explorer, installez un environnement d'exécution Java (JRE). 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 Firefox si vous installez un JRE et configurez le visualiseur de console dans l'interface Web iDRAC6 avant de lancer le visualiseur.
3. Si vous utilisez Internet Explorer® (IE), vérifiez que le navigateur est activé pour télécharger le contenu crypté comme suit :
   - Accédez à Options ou Paramètres d'Internet Explorer et sélectionnez **Outils→ Options Internet → Avancé**.
   - Faites défiler jusqu'à **Sécurité** et décochez l'option suivante :

     Ne pas enregistrer les pages chiffrées sur le disque

4. Si vous utilisez IE pour lancer une session vKVM à l'aide du plug-in Active- X, assurez-vous d'avoir ajouté l'IP ou le nom d'hôte iDRAC6 à la liste **Sites de confiance**. Vous devez également réinitialiser les paramètres personnalisés sur **Moyen-faible** ou modifier les paramètres afin de permettre l'installation de plug-ins Active-X signés.

5. Il est recommandé de configurer la résolution d'affichage de votre moniteur sur au moins 1 280 x 1 024 pixels.

**REMARQUE :** Si votre serveur exécute un système d'exploitation Linux, une console X11 peut ne pas être affichable sur le moniteur local. Appuyez sur <Ctrl><Alt><F1> sur KVM iDRAC6 pour commuter Linux vers une console de texte.

**REMARQUE :** Vous pouvez occasionnellement rencontrer l'erreur de compilation de script Java suivante : « Expected: ; » (Attendu : ;). Pour résoudre ce problème, réglez les paramètres réseau afin d'utiliser une « connexion directe » dans JavaWebStart : « Edition->Préférences->Général->Paramètres réseau » et sélectionnez « Connexion directe » à la place de « Utiliser les paramètres du navigateur ».

## Effacer la mémoire cache de votre navigateur

Si vous rencontrez des problèmes lors de l'utilisation de vKVM (erreurs hors plage, problèmes de synchronisation, etc.), effacez la mémoire cache du navigateur pour supprimer les anciennes versions du visualiseur susceptibles d'être stockées sur le système, puis réessayez.

Pour supprimer les anciennes versions du visualiseur Active-X pour IE6, procédez comme suit :

1. Ouvrez l'invite de commande et remplacez le répertoire par WINDOWS\Downloaded Program Files.

2. Exécutez **regsvr32 /u VideoViewer.ocx**.

3. Supprimez les fichiers suivants : AvctKeyboard.dll, AvctVirtualMediaDE.dll, AvctVirtualMediaES.dll, AvctVirtualMediaFR.dll, AvctVirtualMediaJA.dll, AvctVirtualMediaZH.dll, VideoViewerDE.dll, VideoViewerES.dll, VideoViewerFR.dll, VideoViewerJA.dll, VideoViewerZH.dll et VirtualMediaDLL.dll.

4. Supprimez les modules complémentaires *Session Viewer* et/ou *Video Viewer* qui ont été utilisés par Internet Explorer.

Pour supprimer les anciennes versions du visualiseur Active-X pour IE7, procédez comme suit :

1. Fermez Video Viewer et le navigateur Internet Explorer.

2. Ouvrez à nouveau le navigateur Internet Explorer et accédez à **Internet Explorer→ Outils→ Gérer les modules complémentaires** et cliquez sur **Activer ou désactiver les modules complémentaires**. La fenêtre **Gérer les modules complémentaires** s'affiche.

3. Sélectionnez **Modules complémentaires qui ont été utilisés par Internet Explorer** dans le menu déroulant **Afficher**.

4. Supprimez le module complémentaire *Video Viewer*.

Pour supprimer les anciennes versions du visualiseur Active-X pour IE8, procédez comme suit :

1. Fermez Video Viewer et le navigateur Internet Explorer.

2. Ouvrez à nouveau le navigateur Internet Explorer et accédez à **Internet Explorer→ Outils→ Gérer les modules complémentaires** et cliquez sur **Activer ou désactiver les modules complémentaires**. La fenêtre **Gérer les modules complémentaires** s'affiche.

3. Sélectionnez **Tous les modules complémentaires** dans le menu déroulant **Afficher**.

4. Sélectionnez le module complémentaire *Video Viewer* et cliquez sur le lien **Plus d'informations**.

5. Sélectionnez **Supprimer** dans la fenêtre **Plus d'informations**.

6. Fermez les fenêtres **Plus d'informations** et **Gérer les modules complémentaires**.

Pour supprimer les anciennes versions du visualiseur Java sous Windows ou Linux, procédez comme suit :

1. À l'invite de commande, exécutez `javaws-viewer` ou `javaws- uninstall`

2. Le **visualiseur Java Cache** s'affiche.

3. Supprimez les éléments intitulés *Client de redirection de console iDRAC6*.

## Résolutions d'écran prises en charge et taux de rafraîchissement

Le 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 redirection de console dans l'interface Web iDRAC6

Pour configurer la redirection de console dans l'interface Web iDRAC6, effectuez les étapes suivantes :

1. Cliquez sur **Système**→ **Console/Média**→ **Configuration** pour configurer les paramètres de redirection de console iDRAC6.
2. Configurez les propriétés de la redirection de console. Le tableau 10-2 décrit les paramètres de la redirection de console.
3. Lorsque vous avez terminé, cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Consultez le 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. Si cette option est cochée, cela signifie que la redirection de console est activée. L'option par défaut est **Activé**.<br><br>**REMARQUE :** Le fait de cocher ou de décocher l'option **Activé** dès que le KVM virtuel est lancé risque de déconnecter toutes vos sessions de KVM virtuel existantes. |
| **Nombre maximal de sessions** | Affiche le nombre maximal de sessions de redirection de console possibles (1 à 4). Utilisez le menu déroulant pour modifier le nombre maximal de sessions de redirection de console autorisées. Le nombre maximal par défaut est **2**. |
| **Sessions actives** | Affiche le nombre de sessions de consoles actives. Ce champ est en lecture seule. |
| **Port de présence à distance** | Numéro de port réseau utilisé en vue de la connexion 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. Le port par défaut est **5900**.<br><br>**REMARQUE :** Le fait de modifier la valeur **Port de présence à distance** dès que le KVM virtuel est lancé risque de déconnecter toutes vos sessions de KVM virtuel existantes. |
| **Cryptage vidéo activé** | **Coché** indique que le cryptage vidéo est activé. Tout le trafic à destination du port vidéo est crypté.<br><br>**Décoché** indique que le cryptage vidéo est désactivé. Le trafic à destination du port vidéo n'est pas crypté.<br><br>La valeur par défaut est **Crypté. La désactivation du cryptage peut améliorer les performances sur les réseaux plus lents.**<br><br>**REMARQUE :** Le fait d'activer ou de désactiver l'option **Cryptage vidéo activé** dès que le KVM virtuel est lancé risque de déconnecter toutes vos sessions de KVM virtuel existantes. |
| **Vidéo locale du serveur activée** | Si cette case est cochée, cela signifie que la sortie vers le moniteur KVM iDRAC6 est désactivée lors de la redirection de console. Ceci assure que les tâches que vous effectuez avec la **redirection de console** ne sont pas visibles sur le moniteur local du serveur géré. |
| **Type de plug-in** | Type de plug-in à configurer.<br><br>**Natif** (ActiveX pour Windows® et le plug-in Java pour Linux) : le visualiseur ActiveX fonctionne uniquement sur Internet Explorer®.<br><br>Java : un visualiseur Java est lancé. |

**REMARQUE :** Pour obtenir des informations sur l'utilisation du média virtuel avec la redirection de console, consultez « Configuration et utilisation du média virtuel ».

Les boutons répertoriés dans le tableau 10-3 sont disponibles sur la page **Configuration**.

**Tableau 10-3. Boutons de la page Configuration**

| Bouton | Définition |
|---|---|
| **Imprimer** | Imprime la page |
| **Actualiser** | Recharge la page **Configuration** |

| **Appliquer** | Enregistre tout nouveau paramètre ou tout paramètre modifié |
|---|---|

## Ouverture d'une session de redirection de console

Lorsque vous ouvrez une session de redirection de console, l'application du visualiseur du KVM virtuel de Dell™ démarre et le bureau du système distant apparaît dans le visualiseur. Grâce à l'application du visualiseur du KVM virtuel, vous pouvez contrôler les fonctions de souris et de clavier du système distant à partir de votre station de gestion locale.

**REMARQUE :** Le lancement de vKVM à partir d'une station de gestion Windows Vista® peut entraîner des messages de redémarrage vKVM. Pour éviter ce problème, définissez les valeurs du délai d'expiration appropriées aux emplacements suivants : **Panneau de commande→ Options d'alimentation→ Economiseur d'énergie→ Paramètres avancés→ Disque dur→ Eteindre le disque dur après <délai_d'expiratione>** et dans le **Panneau de commande→ Options d'alimentation→ Haute performance→ Paramètres avancés→ Disque dur→ Eteindre le disque dur après <délai_d'expiration>**.

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

1. Cliquez sur **Système→ Console/Média→ Redirection de console et média virtuel**.
2. Servez-vous des informations de tableau 10-4 pour vérifier qu'une session de redirection de console est disponible.

   Pour reconfigurer les valeurs des propriétés affichées, consultez « Configuration de la redirection de console dans l'interface Web iDRAC6 ».

**Tableau 10-4. Redirection de console**

| Propriété | Description |
|---|---|
| **Redirection de console activée** | Oui/Non (cochée\non cochée) |
| **Cryptage vidéo activé** | Oui/Non (cochée\non cochée) |
| **Nombre maximal de sessions** | Affiche le nombre maximal de sessions de redirection de console prises en charge. |
| **Sessions actives** | Affiche le nombre actuel de sessions de redirection de console actives. |
| **Vidéo locale du serveur activée** | Oui = Activé ; non = Désactivé. |
| **Port de présence à distance** | Numéro de port réseau utilisé en vue de la connexion 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. |
| **Type de plug-in** | Affiche le type de plug-in que vous avez sélectionné à la page **Configuration**.<br><br>**REMARQUE :** Pour les plateformes Windows 64 bits, le plug-in Active-X d'authentification iDRAC6 ne s'installera pas correctement si une version 64 bits du « progiciel redistribuable Microsoft Visual C++ 2005 » est déployée. Pour installer et exécuter le plug-in Active-X correctement, déployez la version 32 bits du « progiciel redistribuable Microsoft Visual C++ 2005 SP1 (x86) ». Ce progiciel est requis pour lancer la session vKVM sur un navigateur Internet Explorer. |

**REMARQUE :** Pour obtenir des informations sur l'utilisation du média virtuel avec la redirection de console, consultez « Configuration et utilisation du média virtuel ».

Les boutons répertoriés dans le tableau 10-5 sont disponibles sur la page **Redirection de console et média virtuel**.

**Tableau 10-5. Boutons de la page Redirection de console et média virtuel**

| Bouton | Définition |
|---|---|
| **Actualiser** | Recharge la page **Redirection de console et média virtuel**. |
| **Lancer le visualiseur** | Ouvre une session de redirection de console sur le système distant ciblé. |
| **Imprimer** | Imprime la page **Redirection de console et média virtuel**. |

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

   **REMARQUE :** Plusieurs boîtes de message peuvent apparaître après le lancement de l'application. Afin d'empêcher l'accès non autorisé à l'application, naviguez au sein de ces boîtes de message dans les trois minutes. 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 iDRAC6.

4. Deux pointeurs de souris apparaissent dans la fenêtre du visualiseur : un pour le système distant et l'autre pour votre système local. Vous pouvez les

remplacer par un curseur unique en sélectionnant l'option **Curseur unique** sous **Outils** dans le menu KVM iDRAC6.

---

## Utilisation de KVM iDRAC6 (Video Viewer)

KVM iDRAC6 (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, KVM iDRAC6 démarre dans une fenêtre séparée.

**REMARQUE :** Si le serveur distant est éteint, le message **Aucun signal** s'affiche.

KVM iDRAC6 fournit divers réglages de commandes tels que la synchronisation de la souris, les instantanés, les macros de clavier et l'accès au média virtuel. Pour plus d'informations sur ces fonctions, cliquez sur **Système→ Console/Média** puis sur **Aide sur la page** d'IUG **Redirection de console et média virtuel**.

Lorsque vous démarrez une session de redirection de console et que KVM iDRAC6 apparaît, il est possible que vous ayez à synchroniser les pointeurs de souris.

Le 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 |
|---|---|---|
| Icône « broche » | SO | Cliquez sur l'icône « broche » pour verrouiller la barre de menus KVM iDRAC6. Cela empêche le masquage automatic<br><br>**REMARQUE :** Cette opération s'applique uniquement au visualiseur Active-X, et non au plug-in Java. |
| Média virtuel | Lancer le média virtuel | La **session de média virtuel** s'affiche et répertorie les périphériques disponibles en vue du mappage dans la fenêtre périphérique, cochez l'option dans la colonne **Mappé** du tableau. Le périphérique sera mappé au serveur à ce stade case.<br><br>Le bouton **Détails** affiche un volet qui répertorie les périphériques virtuels et qui affiche également l'activité de lectu chaque périphérique. |
| Outils | Options de session | La fenêtre Options de sessions fournit des réglages de commandes Session Viewer supplémentaires. Cette fenêtre **Souris**.<br><br>Vous pouvez contrôler le **Mode de transmission au clavier** depuis l'onglet Général. Sélectionnez **Transmettre toute cible** pour transmettre les séquences de touches de votre station de gestion au système distant.<br><br>L'onglet Souris contient deux sections : **Curseur unique** et **Accélération de la souris**. La fonctionnalité **Curseur uni** un décalage des problèmes d'alignement de la souris sur certains systèmes d'exploitation distants. Dès que le visua **unique**, le pointeur de la souris est piégé dans la fenêtre du visualiseur. Appuyez sur la touche d'arrêt pour quitter pour sélectionner la touche qui sortira du mode Curseur unique.<br><br>La fonctionnalité **Accélération de la souris** optimise les performances de la souris selon le système d'exploitation q |
| | Curseur unique | Active le mode curseur unique dans le visualiseur. Dans ce mode, le curseur client est masqué si bien que seul le cu curseur client est également piégé dans le cadre du visualiseur. L'utilisateur ne pourra pas utiliser le curseur hors d qu'il n'aura pas appuyé sur la **touche d'arrêt** spécifiée dans la fenêtre **Options de session**, onglet **Souris**. |
| | Statistiques | Cette option de menu lance une boîte de dialogue qui affiche les statistiques de performances du visualiseur. Les v suivantes :<br><br>- Fréquence des trames<br>- Bande passante<br>- Compression<br>- Fréquence des paquets |
| Fichier | Saisir dans un fichier | Saisit l'écran du système distant actuel dans un fichier **.bmp** sous Windows ou dans un fichier **.png** sous Linux. Une que vous puissiez enregistrer le fichier dans un emplacement spécifié.<br><br>**REMARQUE :** Le format de fichier **.bmp** sous Windows ou **.png** sous Linux s'appliquent uniquement au plug-in natif. en charge les formats de fichier **.jpg** et **.jpeg**. |
| | Quitter | Lorsque vous n'avez plus besoin d'utiliser la console et que vous avez fermé la session (en suivant la procédure de distant), sélectionnez **Quitter** dans le menu **Fichier** pour fermer la fenêtre **KVM iDRAC6**. |
| | Macros | Lorsque vous sélectionnez une macro ou saisissez son raccourci clavier, l'action s'exécute sur le système distant.<br><br>KVM iDRAC6 fournit les macros suivantes :<br><br>- Alt+Ctrl+Suppr<br>- Alt+Tab<br>- Alt+Échap<br>- Ctrl+Échap<br>- Alt+Espace<br>- Alt+Entrée<br>- Alt+Tiret<br>- Alt+F4<br>- ImprÉcran<br>- Alt+Impr. écran<br>- F1 |

| | | |
|---|---|---|
| | | ı Pause<br>ı Tab<br>ı Ctrl+Entrée<br>ı Syst<br>ı Alt+Maj gauche+Maj droit+Échap<br>ı Ctrl+Alt+Retour arrière<br>ı Alt+F? (Où F? représente les touches F1à F12)<br>ı Ctrl+Alt+F? (Où F? représente les touches F1à F12) |
| Alimentation | Allumer le système | Met le système sous tension. |
| | Arrêter le système | Arrête le système. |
| | Arrêt normal | Arrête le système. |
| | Réinitialiser le système (démarrage à chaud) | Réinitialise le système sans le mettre hors tension. |
| | Exécuter un cycle d'alimentation du système (démarrage à froid) | Met le système hors tension, puis le redémarre. |
| Aide | Contenu et index | Fournit des instructions sur la façon d'afficher l'aide en ligne. |
| | À propos de KVM iDRAC6 | Affiche la version de **KVM iDRAC6**. |

## Désactivation ou activation de la vidéo locale du serveur

Vous pouvez configurer iDRAC6 pour interdire les connexions KVM iDRAC6 avec l'interface Web iDRAC6.

Si vous souhaitez vous assurer que vous disposez d'un accès exclusif à la console de serveur géré, vous devez désactiver la console locale *et reconfigurer le* **nombre maximal de sessions** sur 1 sur la **page Configuration de la redirection de console**.

**REMARQUE :** Si vous désactivez (éteignez) la vidéo locale sur le serveur, le moniteur, le clavier et la souris connectés à KVM iDRAC6 sont toujours activés.

Pour désactiver ou activer la console locale, procédez comme suit :

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session sur iDRAC6.
2. Cliquez sur **Système**→ **Console/Média**→ **Configuration**.
3. Pour désactiver (éteindre) la vidéo locale sur le serveur, décochez la case **Vidéo locale du serveur activée** de la page **Configuration,** puis cliquez sur **Appliquer**. La valeur par défaut est Désactivé.

   **REMARQUE :** Si la vidéo locale du serveur est activée, comptez 15 secondes pour qu'il se désactive.

4. Pour activer (allumer) la vidéo locale sur le serveur, cochez la case **Vidéo locale du serveur activée** de la page **Configuration,** puis cliquez sur **Appliquer**.

---

# Lancement de vKVM et du média virtuel à distance

Vous pouvez lancer vKVM/le média virtuel en saisissant une URL unique dans un navigateur pris en charge au lieu de le lancer depuis l'IUG Web iDRAC6. Selon la configuration de votre système, vous passerez par le processus d'authentification manuelle (page d'ouverture de session) ou vous serez dirigé vers le visualiseur vKVM/média virtuel automatiquement.

**REMARQUE :** Internet Explorer prend en charge les ouvertures de session locales, Active Directory (AD), par carte à puce (SC) et par connexion directe (SSO). Firefox prend uniquement en charge les ouvertures de session locales et Active Directory.

## Format d'URL

Si vous saisissez le `lien<IP>/console` dans le navigateur, il vous sera peut-être demandé d'effectuer la procédure d'ouverture de session manuelle normale, selon la configuration d'ouverture de session. Si SSO n'est pas activée et que l'ouverture de session locale, AD ou par carte à puce l'est, la page d'ouverture de session correspondante s'affiche. Si l'ouverture de session réussit, le visualiseur vKVM/vMedia n'est pas lancé. À la place, vous êtes redirigé vers la page d'accueil de l'IUG iDRAC6.

## Scénarios d'erreurs généraux

Le tableau 10-7 répertorie les scénarios d'erreurs généraux, les raisons de ces erreurs et le comportement d'iDRAC6.

**Tableau 10-7. Scénarios d'erreurs**

| Scénarios d'erreurs | Raison | Comportement |
|---|---|---|

| | | |
|---|---|---|
| L'ouverture de session a échoué | Vous avez saisi un nom d'utilisateur non valide ou un mot de passe incorrect. | Comportement identique lorsque ***https://<IP>*** est spécifié et l'ouverture de session échoue. |
| Carte iDRAC6 Enterprise non présente | La carte iDRAC6 Enterprise n'est pas présente. Par conséquent, la fonctionnalité KVM/média virtuel n'est pas disponible. | Le visualiseur KVM iDRAC6 n'est pas lancé. Vous redirige vers la page d'accueil de l'IUG iDRAC6. |
| Privilèges insuffisants | Vous ne disposez pas des privilèges de redirection de console et de média virtuel. | Le visualiseur KVM iDRAC6 n'est pas lancé et vous êtes redirigé vers la page d'IUG de configuration de la console/du média. |
| Redirection de console désactivée | La redirection de console est désactivée sur votre système. | Le visualiseur KVM iDRAC6 n'est pas lancé et vous êtes redirigé vers la page d'IUG de configuration de la console/du média. |
| Paramètres d'URL inconnus détectés | L'URL que vous avez saisie contient des paramètres non définis. | Le message Page introuvable (404) s'affiche. |

## Questions les plus fréquentes concernant la redirection de console

Le tableau 10-8 répertorie les questions les plus fréquentes et les réponses correspondantes.

**Tableau 10-8. Utilisation de la redirection de console : questions les plus fréquentes**

| Question | Réponse |
|---|---|
| vKVM ne se déconnecte pas lors de la fermeture de la session de l'IUG Web hors bande. | Les sessions vKVM et vMedia demeurent actives, même si la session Web est fermée. Fermez les applications de visualiseur vMedia et vKVM afin de fermer la session correspondante. |
| Est-ce qu'une nouvelle session vidéo de la console distante 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 être désactivée après une requête pour la désactiver ? | Ceci permet à l'utilisateur local d'agir avant que la vidéo ne soit désactivée. |
| Est-ce qu'il y a un délai quand la vidéo locale est activée ? | Non, une fois la requête d'**activation** de la vidéo locale reçue par iDRAC6, la vidéo est activée instantanément. |
| Est-ce que l'utilisateur local peut également désactiver la vidéo ? | Lorsque la console locale est désactivée, l'utilisateur local ne peut pas désactiver la vidéo. |
| Est-ce que l'utilisateur local peut également activer la vidéo ? | Lorsque la console locale est désactivée, l'utilisateur local ne peut pas activer la vidéo. |
| La désactivation de la vidéo locale désactive-t-elle aussi le clavier et la souris locaux ? | Non. |
| La désactivation de la console locale désactive-t-elle la vidéo sur la session de la console distante ? | Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de la console distante. |
| Quels sont les privilèges nécessaires à un utilisateur iDRAC6 pour activer ou désactiver la vidéo locale du serveur ? | Tout utilisateur disposant de privilèges de configuration iDRAC6 peut activer ou désactiver la console locale. |
| Comment connaître la condition actuelle de la vidéo locale du serveur ? | La condition est affichée dans la page **Configuration de la redirection de console** de l'interface Web iDRAC6.<br><br>La commande CLI RACADM **racadm getconfig -g cfgRacTuning** affiche la condition dans l'objet **cfgRacTuneLocalServerVideo**. |
| Je n'arrive pas à voir le bas de l'écran système à partir de la fenêtre Redirection de console. | Assurez-vous que la résolution du moniteur de la station de gestion est définie sur 1280 x 1024. Essayez également d'utiliser les barres de défilement du client KVM iDRAC6. |
| La fenêtre de la console est tronquée. | Le visualiseur de console sous Linux requiert un jeu de caractères UTF-8. Vérifiez vos paramètres régionaux et réinitialisez le jeu de caractères si nécessaire. |
| Pourquoi la souris ne se synchronise-t-elle pas sous la console de texte Linux dans **Dell Unified Server Configurator (USC), Dell Lifecycle Controller** ou **Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE**) ? | Le KVM virtuel requiert le 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.<br><br>Vérifiez que l'option **Curseur unique sous Outils** dans le menu KVM iDRAC6 est sélectionnée sur le client KVM iDRAC6. Le mode à deux curseurs est défini par défaut. |
| 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 sur lequel la 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.<br><br>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 la condition Verr Num sur le serveur distant ? | Lors d'un accès via iDRAC6, l'indicateur Verr Num sur la station de gestion ne correspond pas nécessairement à l'état Verr Num sur le serveur distant. L'état Verr Num dépend du paramètre sur le serveur distant lorsque la 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 ? | Il est recommandé de recourir à une connexion de 5 Mo/s. pour des performances optimales. Une connexion de 1 Mo/s suffit pour une performance minimale. |
| Quelle est la configuration système minimale requise pour que ma station de gestion exécute la redirection de console ? | La station de gestion nécessite un processeur Intel® Pentium® III 500 MHz avec au moins 256 Mo de RAM. |
| Pourquoi est-ce qu'un message **Aucun signal** s'affiche dans Video Viewer KVM iDRAC6 ? | Ce message peut s'afficher lorsque le plug-in KVM virtuel iDRAC6 ne reçoit pas la vidéo du bureau du serveur distant. En règle générale, cette situation a lieu lorsque le serveur distant est éteint. Parfois, le message peut s'afficher en raison de problèmes de réception de la vidéo du bureau du serveur distant. |
| Pourquoi est-ce qu'un message **Hors plage** s'affiche dans le Video Viewer KVM iDRAC6 ? | Ce message peut s'afficher si un paramètre nécessaire à la capture de la vidéo se situe au-delà de la plage dans laquelle iDRAC6 peut capturer la vidéo. Des paramètres tels que la résolution de l'affichage ou un taux de rafraîchissement trop élevés peuvent entraîner une condition hors plage. En règle générale, la plage maximale des paramètres est définie par des limitations physiques telles que la taille de la mémoire vidéo ou la bande passante. |

---

Retour à la page du sommaire