

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

[Présentation d'iDRAC6 Enterprise](#)

[Configuration d'iDRAC6 Enterprise](#)

[Configuration de la station de gestion](#)

[Configuration du serveur géré](#)

[Configuration d'iDRAC6 Enterprise via l'interface Web](#)

[Utilisation du service d'annuaire iDRAC6](#)

[Configuration d'iDRAC6 pour la connexion directe et l'ouverture de session par carte à puce](#)

[Visualisation de la configuration et de l'intégrité du serveur géré](#)

[Configuration et utilisation des communications série sur le LAN](#)

[Utilisation de la console virtuelle de l'interface utilisateur](#)

[Configuration de la carte SD vFlash et gestion des partitions vFlash](#)

[Configuration et utilisation du média virtuel](#)

[Utilisation de l'interface de ligne de commande RACADM](#)

[Contrôle et gestion de l'alimentation](#)

[Utilisation d'iDRAC6 Enterprise Interface de ligne de commande SM-CLI](#)

[Utilisation de l'interface WS-MAN](#)

[Déploiement de votre système d'exploitation via iVMCLI](#)

[Utilisation de l'utilitaire de configuration iDRAC6](#)

[Récupération et dépannage du système géré](#)

Remarques et précautions

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

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

Les informations contenues dans ce document sont sujettes à modification sans préavis.
© 2010 Dell Inc. Tous droits réservés.

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

Marques mentionnées dans ce document : Dell™, le logo DELL™, OpenManage™ et PowerEdge™ sont des marques de Dell Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, Windows Vista®, MS-DOS™, ActiveX™ et Active Directory® sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Red Hat® et Red Hat Enterprise Linux® sont des marques déposées de Red Hat, Inc. aux États-Unis et dans d'autres pays. Novell® et SUSE® sont des marques déposées de Novell, Inc. aux États-Unis et dans d'autres pays. Intel® et Pentium® sont des marques déposées de Intel Corporation aux États-Unis et dans d'autres pays. UNIX® est une marque déposée de The Open Group aux États-Unis et dans d'autres pays. Thawte® est une marque déposée de Thawte et de ses filiales aux États-Unis et dans les pays étrangers. VeriSign® est une marque déposée de VeriSign, Inc. et de ses filiales aux États-Unis et dans les pays étrangers. Sun™ et Java™ sont des marques ou des marques déposées de Sun Microsystems, Inc. ou de ses filiales aux États-Unis et dans d'autres pays. Mozilla® et Firefox® sont des marques déposées de Mozilla Foundation.

Copyright 1998-2009 The OpenLDAP Foundation. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire, avec ou sans modification, ne sont permises que selon les termes de la licence publique OpenLDAP. Une copie de cette licence est disponible dans le fichier LICENSE qui se trouve dans le répertoire de haut niveau de la distribution ou à l'adresse www.OpenLDAP.org/license.html. OpenLDAP est une marque déposée de The OpenLDAP Foundation. Il se peut que certains fichiers individuels et/ou logiciels fournis par des tiers soient sous copyright et qu'ils soient sujets à des restrictions supplémentaires. Ce produit est dérivé de la distribution LDAP v3.3 de l'Université du Michigan. Ce produit contient aussi des produits dérivés de sources publiques. Les informations sur OpenLDAP sont disponibles sur www.openldap.org/. Parties de Copyright 1998-2004 Kurt D. Zeilenga. Parties de Copyright 1998-2004 Net Boolean Incorporated. Parties de Copyright 2001-2004 IBM Corporation. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire, avec ou sans modification, ne sont permises que selon les termes de la licence publique OpenLDAP. Parties de Copyright 1999-2003 Howard Y.H. Chu. Parties de Copyright 1999-2003 Symas Corporation. Parties de Copyright 1998-2003 Hallvard B. Furuseth. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire, avec ou sans modification, sont permises tant que cet avis est conservé. Les noms des détenteurs de copyright ne peuvent pas être utilisés pour approuver ou promouvoir des produits dérivés de ce logiciel sans leur autorisation préalable par écrit. Ce logiciel est fourni « tel quel » sans garantie explicite ou tacite. Parties de Copyright (c) 1992-1996 Membres du conseil de l'Université du Michigan. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire sont permises tant que cet avis est conservé et que l'Université du Michigan à Ann Arbor reçoit les crédits qui lui sont dus. Le nom de l'université ne peut pas être utilisé pour approuver ou promouvoir des produits dérivés de ce logiciel sans son autorisation préalable par écrit. Ce logiciel est fourni « tel quel » sans garantie explicite ou tacite.

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

Juillet 2010

[Retour à la page du sommaire](#)

Présentation d'iDRAC6 Enterprise

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Certification « IPv6 Ready Logo »](#)
- [Fonctionnalités de sécurité iDRAC6](#)
- [iDRAC6 Enterprise et média vFlash](#)
- [Plates-formes prises en charge](#)
- [Systèmes d'exploitation pris en charge](#)
- [Navigateurs Web pris en charge](#)
- [Connexions d'accès à distance prises en charge](#)
- [Ports iDRAC6](#)
- [Autres documents utiles](#)

Integrated Dell Remote Access Controller (iDRAC6) Enterprise 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 puce » intégré pour le système de contrôle/surveillance à distance et coexiste sur la carte système avec le serveur Dell PowerEdge géré. Le système d'exploitation du serveur exécute les applications ; l'iDRAC6 surveille et gère l'environnement et l'état du serveur en dehors du système d'exploitation.

Vous pouvez configurer iDRAC6 pour qu'il envoie des alertes par e-mail ou interruption SNMP (Simple Network Management Protocol [protocole simplifié de gestion de réseau]) en cas d'avertissement ou d'erreur. Pour vous aider à diagnostiquer la cause d'un plantage du système, l'iDRAC6 peut consigner des données d'événement et capturer une image de l'écran lorsqu'il détecte un plantage du système.

Les serveurs gérés sont installés dans une enceinte (châssis) du système Dell M1000e avec des blocs d'alimentation modulaires, des ventilateurs et un contrôleur CMC (Chassis Management Controller). CMC surveille et gère tous les composants installés dans le châssis. Un CMC redondant peut être ajouté pour assurer un basculement à chaud si le CMC principal échoue. Le châssis permet d'accéder aux périphériques iDRAC6 via son écran LCD, des connexions de console locale et son interface Web. Chaque lame d'un châssis possède un iDRAC6. Au total, 16 lames peuvent être installées dans le M1000e.

Toutes les connexions réseau à iDRAC6 sont acheminées via les interfaces réseau CMC (port de connexion RJ45 CMC nommé « GB1 »). CMC achemine le trafic vers les périphériques iDRAC6 par le biais d'un réseau privé interne. Ce réseau de gestion privé se trouve hors du chemin d'accès des données du serveur et hors du contrôle du système d'exploitation, autrement dit *hors bande*. Les interfaces réseau *intra-bandes* du serveur géré sont accessibles via les modules d'E/S (IOM) installés dans le châssis.

 **REMARQUE :** Il est recommandé d'isoler ou de séparer le réseau de gestion du châssis, utilisé par iDRAC6 et CMC, de votre ou vos réseaux de production. Le mélange des trafics des réseaux de gestion, de production et applicatif peut entraîner une congestion ou une saturation du réseau et ainsi des retards de communication du CMC et d'iDRAC6. Ces retards risquent d'entraîner un comportement imprévisible du châssis, tel qu'un affichage du CMC indiquant qu'iDRAC6 est hors ligne alors qu'il fonctionne correctement. Ceci peut également entraîner un autre comportement imprévisible.

L'interface réseau iDRAC6 est désactivée par défaut. Vous devez la configurer pour pouvoir accéder à iDRAC6. Une fois iDRAC6 activé et configuré sur le réseau, il est accessible à l'adresse IP qui lui a été attribuée via l'interface Web iDRAC6, via Telnet ou SSH, ainsi que via les protocoles de gestion de réseau pris en charge, comme IPMI (Interface de gestion de plateforme intelligente).

Certification « IPv6 Ready Logo »

La mission du comité IPv6 Ready Logo est de définir les spécifications de test de conformité et d'interopérabilité IPv6, de donner accès à des outils d'auto-test et d'accorder le logo « IPv6 Ready ».

L'iDRAC6 est certifié « IPv6 Ready Logo Phase 2 » et l'ID du logo est **02-C-000380**. Pour plus d'informations sur le programme IPv6 Ready Logo, rendez-vous sur le site <http://www.ipv6ready.org/>.

Fonctionnalités de sécurité iDRAC6

- 1 Authentification des utilisateurs via Microsoft Active Directory, le service d'annuaire LDAP générique ou des réf. utilisateur et des mots de passe administrés localement
- 1 Authentification bifactorielle assurée par la fonctionnalité d'ouverture de session par carte à puce. L'authentification bifactorielle est basée sur ce que possèdent les utilisateurs (la carte à puce) et sur ce qu'ils *connaissent* (le NIP)
- 1 Autorisation basée sur les rôles, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- 1 Configuration de la réf. utilisateur et du mot de passe
- 1 Interfaces SM-CLP et Web prenant en charge le cryptage 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté) à l'aide de la norme SSL 3.0
- 1 Configuration du délai d'expiration de la session (en secondes)
- 1 Ports IP configurables (si applicable)
- 1 Secure Shell (SSH), qui utilise une couche de transport cryptée pour une sécurité plus élevée
- 1 Nombre maximal d'échecs d'ouverture de session par adresse IP, avec blocage de l'ouverture de session à partir de cette adresse IP lorsque la limite est dépassée
- 1 Plage d'adresses IP client configurable pour les clients se connectant à iDRAC6

iDRAC6 Enterprise et média vFlash

iDRAC6 Enterprise fournit des logements de carte SD pour le média vFlash. Pour plus d'informations sur iDRAC6 Enterprise et le média vFlash, consultez le

Manuel du propriétaire du matériel à l'adresse support.dell.com/manuals.

[Tableau 1-1](#) répertorie les fonctionnalités disponibles pour iDRAC6 Enterprise et le média vFlash.

Tableau 1-1. Liste de fonctionnalités iDRAC6

Fonctionnalité	iDRAC6 Enterprise	iDRAC6 Enterprise avec média vFlash
Prise en charge de l'interface et des normes		
IPMI 2.0	✓	✓
Interface utilisateur Web	✓	✓
SNMP	✓	✓
WS-MAN	✓	✓
SM-CLP	✓	✓
Ligne de commande RACADM	✓	✓
Connectivité		
Modes réseau Partagé/Basculement	✓	✓
IPv4	✓	✓
Marquage VLAN	✓	✓
IPv6	✓	✓
DNS dynamique	✓	✓
NIC dédié	✓	✓
Sécurité et authentification		
Autorisation basée sur les rôles	✓	✓
Utilisateurs locaux	✓	✓
Active Directory	✓	✓
Authentification bifactorielle	✓	✓
Connexion directe	✓	✓
Cryptage SSL	✓	✓
Gestion et conversion à distance		
Mise à jour de micrologiciel à distance	✓	✓
Contrôle de l'alimentation du serveur	✓	✓
Série sur le réseau local (avec proxy)	✓	✓
Série sur le réseau local (sans proxy)	✓	✓
Plafonnement de l'alimentation	✓	✓
Capture de l'écran de la dernière panne	✓	✓
Capture au démarrage	✓	✓
Média virtuel	✓	✓
Partage de fichiers à distance	✓	✓
Console virtuelle	✓	✓
Partage de la console virtuelle	✓	✓
vFlash	✗	✓
Surveillance		
Surveillance et alertes des capteurs	✓	✓
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	✓	✓
Journal système distant	✓	✓
✓ = pris en charge ; ✗ = non pris en charge		

Plates-formes prises en charge

Pour connaître les dernières plates-formes 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 connaître les dernières informations, 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 connaître les dernières informations, 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 défauts de sécurité, la prise en charge de SSL 2.0 a été abandonnée. Assurez-vous que votre navigateur est configuré pour activer SSL 3.0

Connexions d'accès à distance prises en charge

[Tableau 1-2](#) répertorie les fonctionnalités de connexion.

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

Connexion	Fonctionnalités
NIC iDRAC6	<ul style="list-style-type: none"> 1 Ethernet 10 Mbits/s/100 Mb/s/1 Gbits/s via le port Ethernet Gb CMC. 1 Prise en charge de DHCP. 1 Interruptions SNMP et notifications d'événements par e-mail. 1 Les commandes de l'environnement SM-CLP et RACADM pour des opérations telles que la configuration d'iDRAC6, le démarrage du système, la réinitialisation, la mise sous tension ainsi que les commandes d'arrêt sont prises en charge via SSH et Telnet. 1 Prise en charge des utilitaires IPMI, tels qu'IPMITool et ipmish.

Ports iDRAC6

[Tableau 1-3](#) répertorie les ports sur lesquels iDRAC6 écoute les connexions. [Tableau 1-4](#) identifie les ports qu'iDRAC6 utilise en tant que client. Ces informations sont requises pour ouvrir des pare-feu pour pouvoir accéder à distance à un iDRAC6.

PRÉCAUTIONS : iDRAC6 ne recherche pas les conflits entre les ports configurables. Lors de la définition des configurations de port, vérifiez que les attributions de port n'entrent pas en conflit entre elles.

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

Numéro de port	Fonction
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+

3668, 3669	Service de média virtuel
3670, 3671	Service de média virtuel sécurisé
3672	Service vFlash
5900*	Clavier/Souris de la console virtuelle
5901*	Vidéo de la console virtuelle
5988*	Utilisé pour WSMAN
* 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. Vous pouvez accéder à ces guides disponibles sur le site Web du support de Dell à l'adresse support.dell.com/manuals. Sur la page **Manuels**, cliquez sur **Logiciels** → **Systems Management**. Cliquez sur le lien du produit approprié sur le côté droit pour accéder aux documents.

- 1 L'aide en ligne d'iDRAC6 fournit des informations sur l'utilisation de l'interface Web.
- 1 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.
- 1 Le *Guide d'installation de Dell OpenManage Server Administrator* contient des instructions visant à vous aider à installer Dell OpenManage Server Administrator.
- 1 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.
- 1 Le *Guide d'utilisation de Dell Chassis Management Controller* et le *Guide de référence de l'administrateur de Dell Chassis Management Controller* fournissent des informations sur l'utilisation du contrôleur qui gère tous les modules du châssis où réside votre serveur Dell PowerEdge.
- 1 Le *Guide d'utilisation de Dell OpenManage IT Assistant* fournit des informations relatives à l'utilisation d'IT Assistant.
- 1 Le *Guide d'utilisation de Dell Management Console* fournit des informations sur l'utilisation de Dell Management Console.
- 1 Le *Guide d'utilisation de Dell OpenManage Server Administrator* fournit des informations sur l'installation et l'utilisation de Server Administrator.
- 1 Le *Guide d'utilisation des progiciels Dell Update Packages* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Packages dans le contexte de la stratégie de mise à jour de votre système.
- 1 Le *Guide d'utilisation de Dell Lifecycle Controller* fournit des informations sur l'utilitaire Unified Server Configurator (USC), l'utilitaire Unified Server Configurator - Lifecycle Controller Enabled (USC - LCE) et les services distants.
- 1 Les documents *iDRAC6 CIM Element Mapping* et *iDRAC6 SM-CLP Property Database* disponibles dans le centre Dell Enterprise Technology Center à l'adresse www.delltechcenter.com fournissent des informations sur la base de données de propriétés iDRAC6 SM-CLP, les mappages entre les classes WS-MAN et les cibles SM-CLP, et des informations détaillées sur l'implémentation Dell.
- 1 Le *Guide de référence de l'administrateur d'iDRAC6* fournit des informations sur les sous-commandes RACADM, les interfaces RACADM prises en charge ainsi que les groupes de bases de données de propriétés et les définitions d'objets pour iDRAC6 Enterprise sur les serveurs lames et iDRAC6 Enterprise ou Express sur les serveurs en rack et en tour.
- 1 Le *glossaire* fournit des informations sur les termes utilisés dans ce document.

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

- 1 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, consultez la page d'accueil Regulatory Compliance (Conformité à la réglementation) à l'adresse www.dell.com/regulatory_compliance. Les informations sur la garantie se trouvent dans ce document ou dans un document distinct.
- 1 Le *Guide de mise en route* présente les caractéristiques du système, les procédures de configuration et les spécifications techniques.
- 1 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.
- 1 La documentation relative aux logiciels de gestion de systèmes décrit les fonctionnalités, la configuration requise, l'installation et l'utilisation de base du logiciel.
- 1 La documentation du système d'exploitation indique comment installer (au besoin), configurer et utiliser le système d'exploitation.
- 1 La documentation fournie avec les composants achetés séparément indique comment configurer et installer ces options.
- 1 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.

- 1 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.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration d'iDRAC6 Enterprise

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Avant de commencer](#)
- [Interfaces de configuration d'iDRAC6](#)
- [Tâches de configuration](#)
- [Configuration des paramètres réseau via l'interface Web CMC](#)
- [Visualisation des connexions de structure des cartes mezzanines FlexAddress](#)
- [Journal système distant](#)
- [Périphérique de démarrage initial](#)
- [Partage de fichiers distant](#)
- [Module SD interne double](#)
- [Mise à jour du micrologiciel iDRAC6](#)
- [Mise à jour du progiciel de réparation de l'USC](#)
- [Configuration d'iDRAC6 pour l'utiliser avec IT Assistant](#)
- [Utilisation de l'utilitaire de configuration iDRAC6 pour activer la découverte](#)
- [Utilisation de l'interface Web iDRAC6 pour activer la découverte et la surveillance](#)
- [Utilisation d'IT Assistant pour afficher la condition et les événements iDRAC6](#)

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

Avant de commencer

Réunissez les éléments suivants avant de configurer iDRAC6 :

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

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

- 1 Racine du DVD : contient Dell Systems Build and Update Utility, qui fournit des informations de configuration du serveur et d'installation du système
- 1 SYSMGMT : contient les produits Systems Management Software, dont Dell OpenManage Server Administrator

Pour de plus amples informations, consultez le *Guide d'installation de Dell OpenManage Server Administrator* et le *Guide d'installation de Dell OpenManage Management Station Software* disponibles sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Interfaces de configuration d'iDRAC6

Vous pouvez configurer iDRAC6 à l'aide de l'utilitaire de configuration iDRAC6, de l'interface Web iDRAC6, de l'interface Web CMC (Chassis Management Controller), de l'écran LCD du châssis, de la CLI RACADM locale et distante ou de la CLI SM-CLP. La CLI RACADM locale est disponible une fois que vous avez installé le système d'exploitation et le logiciel Dell OpenManage sur le serveur géré. [Tableau 2-1](#) décrit ces interfaces.

Pour renforcer la sécurité, l'accès à la configuration d'iDRAC6 via l'utilitaire de configuration d'iDRAC6 ou la CLI de la RACADM locale peut être désactivé avec une commande RACADM (consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible à l'adresse support.dell.com/manuals) ou depuis l'interface utilisateur (consultez [Activation ou désactivation de l'accès à la configuration locale](#).)

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

Tableau 2-1. Interfaces de configuration

Interface	Description
Configuration d'iDRAC6 Utilitaire	L'utilitaire de configuration d'iDRAC6, auquel il est possible d'accéder au démarrage, est particulièrement utile lors de l'installation d'un nouveau serveur Dell PowerEdge. Utilisez-le pour configurer le réseau et les fonctionnalités de sécurité de base, ainsi que pour activer d'autres fonctionnalités.
Interface Web iDRAC6	L'interface Web iDRAC6 est une application de gestion basée sur un navigateur que vous pouvez utiliser pour gérer iDRAC6 de manière interactive et surveiller le serveur géré. Il s'agit de l'interface principale servant à l'exécution des tâches quotidiennes, comme la surveillance de l'intégrité du système, l'affichage du journal des événements système, la gestion des utilisateurs locaux d'iDRAC6 et le lancement de l'interface Web CMC et des sessions de console virtuelle.
Interface Web CMC	Outre la surveillance et la gestion du châssis, l'interface Web CMC peut être utilisée pour afficher la condition d'un serveur géré, mettre à jour le micrologiciel iDRAC6, configurer les paramètres réseau iDRAC6, se connecter à l'interface Web iDRAC6 et démarrer, arrêter ou réinitialiser le serveur géré.
Écran LCD du châssis	L'écran LCD du châssis contenant iDRAC6 peut être utilisé pour afficher la condition de niveau élevé des serveurs présents dans le châssis. Lors de la configuration initiale de CMC, l'Assistant de configuration vous permet d'activer la configuration DHCP de la mise en réseau iDRAC6.
RACADM locale et distante	L'interface de ligne de commande RACADM locale s'exécute sur le serveur géré. Elle est accessible depuis une session de console virtuelle lancée depuis l'interface Web d'iDRAC6. La RACADM est installée sur le serveur géré lorsque vous installez Dell OpenManage Server Administrator. La RACADM distante est un utilitaire client, exécuté sur une station de gestion. Elle utilise l'interface réseau hors bande pour exécuter des commandes RACADM sur le serveur géré. L'option -r exécute la commande RACADM sur un réseau. Les commandes RACADM permettent d'accéder à quasiment toutes les fonctionnalités iDRAC6. Vous pouvez inspecter les données du capteur, les enregistrements du journal des événements système et les valeurs de condition et de configuration actuelles conservées dans iDRAC6. Vous pouvez modifier les valeurs de configuration iDRAC6, gérer les utilisateurs locaux, activer et désactiver les fonctionnalités et exécuter des fonctions d'alimentation, comme l'arrêt ou le redémarrage du serveur géré.
CLI de l'IVM	L'interface de ligne de commande du média virtuel iDRAC6 (IVMCLI) permet au serveur géré d'accéder au média sur la station de gestion. Elle est particulièrement utile pour développer des scripts permettant d'installer des systèmes d'exploitation sur plusieurs serveurs gérés.

SM-CLP	<p>SM-CLP est la mise en œuvre du protocole de ligne de commande Server Management (SM-CLP) du groupe de travail de gestion de serveur incorporé dans iDRAC6. La ligne de commande SM-CLP est accessible en ouvrant une session sur iDRAC6 à l'aide de Telnet ou de SSH et en tapant <code>smclp</code> à l'invite CLI.</p> <p>Les commandes SM-CLP permettent d'implémenter un sous-ensemble, particulièrement utile, des commandes RACADM locales. Ces commandes sont utiles pour l'écriture de scripts car elles peuvent être exécutées à partir d'une ligne de commande de la station de gestion. La sortie des commandes peut être récupérée dans des formats bien définis, y compris le format XML, facilitant ainsi l'écriture de scripts et l'intégration avec les outils de génération de rapports et de gestion existants.</p>
IPMI	<p>IPMI définit une méthode standard permettant aux sous-systèmes de gestion intégrés, comme iDRAC6, de communiquer avec d'autres systèmes intégrés et d'autres applications de gestion.</p> <p>Vous pouvez utiliser l'interface Web iDRAC6, SM-CLP ou les commandes RACADM pour configurer les filtres d'événements sur plateforme (PEF) et les interruptions d'événements sur plateforme (PET) IPMI.</p> <p>Les PEF obligent iDRAC6 à effectuer des actions spécifiques (par exemple, le redémarrage du serveur géré) lorsqu'une condition est détectée. Les PET ordonnent à iDRAC6 d'envoyer des alertes par e-mail ou IPMI lorsque des événements ou des conditions spécifiés sont détectés.</p> <p>Vous pouvez également utiliser des outils IPMI standard tels que IPMI tool et ipmish avec iDRAC6 lorsque vous activez IPMI sur le LAN.</p>

Tâches de configuration

Cette section est une présentation des tâches de configuration pour la station de gestion, iDRAC6 et le serveur géré. Les tâches à effectuer incluent la configuration d'iDRAC6 afin de pouvoir y accéder à distance, la configuration des fonctionnalités d'iDRAC6 que vous souhaitez utiliser, l'installation du système d'exploitation sur le serveur géré et l'installation de Management Software sur votre station de gestion et sur le serveur géré.

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

 **REMARQUE :** Avant d'effectuer les procédures de configuration du présent guide, les modules CMC et d'E/S doivent être installés dans le châssis et configurés, et le serveur Dell PowerEdge doit être physiquement installé dans le châssis.

Configurer la station de gestion

Configurez une station de gestion en installant le logiciel Dell OpenManage, un navigateur Web et d'autres utilitaires logiciels. Consultez [Configuration de la station de gestion](#).

Configurer la mise en réseau iDRAC6

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

 **REMARQUE :** L'accès à la configuration d'iDRAC6 via l'utilitaire de configuration d'iDRAC6 ou la CLI de la RACADM locale peut être désactivé avec une commande RACADM (consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible à l'adresse support.dell.com/manuals) ou depuis l'interface utilisateur (consultez [Activation ou désactivation de l'accès à la configuration locale](#).)

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

 **REMARQUE :** L'option permettant de configurer le serveur via l'écran LCD est disponible *uniquement* lors de la configuration initiale de CMC. Une fois le châssis déployé, l'écran LCD ne peut pas être utilisé pour reconfigurer iDRAC6.

 **REMARQUE :** L'écran LCD peut être utilisé uniquement pour activer DHCP pour configurer le réseau iDRAC6.

- 1 Écran LCD du châssis : consultez le *Guide d'utilisation du micrologiciel Dell Chassis Management Controller*
- 1 Utilitaire de configuration d'iDRAC6 : consultez [Utilisation de l'utilitaire de configuration iDRAC6](#)
- 1 Interface Web CMC : consultez [Configuration des paramètres réseau via l'interface Web CMC](#)
- 1 RACADM distante et locale : consultez `cfgLanNetworking` dans le *Guide de référence de l'administrateur d'iDRAC6* disponible à l'adresse support.dell.com/manuals

Configurer les utilisateurs iDRAC6

Configurez les utilisateurs locaux iDRAC6 ainsi que leurs droits. iDRAC6 intègre un tableau de seize utilisateurs locaux dans le micrologiciel. Vous pouvez définir les noms d'utilisateur, mots de passe et rôles pour ces utilisateurs.

- 1 Utilitaire de configuration d'iDRAC6 (configure l'utilisateur d'administration uniquement) : consultez [Configuration de l'utilisateur LAN](#)
- 1 Interface Web iDRAC6 : consultez [Ajout et configuration d'utilisateurs iDRAC6](#)
- 1 RACADM distante et locale : consultez [Ajout d'un utilisateur iDRAC6](#)

 **REMARQUE :** Lorsque vous utilisez iDRAC6 dans un environnement Active Directory/de service d'annuaire LDAP générique, vérifiez que vos noms d'utilisateur respectent la convention d'attribution de noms d'Active Directory/de service d'annuaire LDAP générique en vigueur.

Configurer les services d'annuaire

En plus des utilisateurs locaux d'iDRAC6, vous pouvez utiliser Microsoft Active Directory ou le service d'annuaire LDAP générique pour authentifier les ouvertures de session utilisateur sur iDRAC6.

Pour plus d'informations, consultez [Utilisation du service d'annuaire iDRAC6, page 141](#).

Configurer le filtrage IP et le blocage IP

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

- 1 Interface Web iDRAC6 : consultez [Configuration du filtrage IP et du blocage IP](#)
- 1 RACADM : consultez [Configuration du filtrage IP \(plage IP\)](#) et [Configuration du blocage IP](#)

Configurer les événements sur plateforme

Les événements sur plateforme se produisent lorsque iDRAC6 détecte un avertissement ou une condition critique provenant de l'un des capteurs du serveur géré.

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

- 1 Interface Web iDRAC6 : consultez [Configuration des filtres d'événements sur plateforme \(PEF\)](#)
- 1 RACADM : consultez [Configuration de PEF](#)

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

- 1 Interface Web iDRAC6 : consultez [Configuration des interruptions d'événement sur plateforme \(PET\)](#)
- 1 RACADM : consultez [Configuration du PET](#)

Activation ou désactivation de l'accès à la configuration locale

L'accès aux paramètres de configuration critiques, comme la configuration réseau et les privilèges utilisateur, peut être désactivé. Une fois l'accès désactivé, le paramètre persiste d'un réamorçage à l'autre. L'accès en écriture à la configuration est bloqué pour le programme de la RACADM locale et l'utilitaire de configuration iDRAC6 (au démarrage). L'accès Web aux paramètres de configuration est libre et les données de configuration peuvent toujours être visualisées. Pour des informations sur l'interface Web iDRAC6, consultez [Activation ou désactivation de l'accès à la configuration locale](#). Pour les commandes RACADM, consultez `cfgRacTuning` dans le *Guide de référence de l'administrateur d'iDRAC6* disponible à l'adresse support.dell.com/manuals.

Configurer les services iDRAC6

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

- 1 Interface Web iDRAC6 : consultez [Configuration des services iDRAC6](#)
- 1 RACADM : consultez [Configuration de services Telnet et SSH iDRAC6 via la RACADM locale](#)

Configurer le protocole Secure Sockets Layer (SSL)

Configurez le protocole SSL pour Web Server iDRAC6.

- 1 Interface Web iDRAC6 : consultez [Secure Sockets Layer \(SSL\)](#)
- 1 RACADM : consultez `cfgRacSecurity`, `sslcsrngen`, `sslcertupload`, `sslcertdownload` et `sslcertview` dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Configurer le média virtuel

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

- 1 Interface Web iDRAC6 : consultez [Configuration et utilisation du média virtuel](#)
- 1 Utilitaire de configuration d'iDRAC6 : consultez [Configuration du média virtuel](#)

Configurer une carte de média vFlash

Installez et configurez une carte de média vFlash pour utilisation avec iDRAC6.

- 1 Interface Web iDRAC6 et utilisation de la RACADM : consultez [Configuration de la carte SD vFlash et gestion des partitions vFlash](#)

Installer le logiciel Managed Server

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

- 1 Console virtuelle : consultez [Installation du logiciel sur le serveur géré](#)
- 1 iVMCLI : consultez [Utilisation de l'utilitaire d'interface de ligne de commande de média virtuel](#)

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

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

- 1 Serveur géré : consultez [Configuration du serveur géré pour la capture de l'écran de la dernière panne](#) et [Désactivation de l'option Redémarrage automatique de Windows](#)

Configuration des paramètres réseau via l'interface Web CMC

 **REMARQUE :** Vous devez disposer du privilège Administrateur et configuration du châssis pour pouvoir configurer les paramètres réseau iDRAC6 depuis CMC.

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

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

Lancement de l'interface Web iDRAC6 à partir de CMC

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

Pour lancer iDRAC6 depuis CMC :

1. Ouvrez une session sur l'interface Web CMC.
2. Dans l'arborescence du système, sélectionnez **Présentation des serveurs**. L'écran **Condition des serveurs** affiche la liste des serveurs disponibles.
3. Cliquez sur **iDRAC** pour le serveur que vous voulez gérer. L'interface utilisateur d'iDRAC est lancée dans une nouvelle fenêtre de navigateur.

Pour lancer l'interface Web iDRAC6 pour un serveur unique depuis CMC :

1. Ouvrez une session sur l'interface Web CMC.
2. Développez **Présentation des serveurs** dans l'arborescence du système. Tous les serveurs s'affichent dans la liste développée **Serveurs**.
3. Cliquez sur le serveur dont vous souhaitez afficher les informations. L'écran **Condition des serveurs** pour le serveur que vous avez sélectionné apparaît.
4. Cliquez sur **Lancer l'interface utilisateur iDRAC6**.

Connexion directe

La fonctionnalité de connexion directe vous permet de lancer l'interface Web iDRAC6 depuis CMC sans avoir à ouvrir une session une deuxième fois. Les stratégies de connexion directe sont décrites ci-dessous.

- 1 Un utilisateur CMC pour lequel **Server Administrator** est défini sous **Privilèges utilisateur** ouvrira automatiquement une session sur l'interface Web iDRAC6 à l'aide de la connexion directe. Une fois la session ouverte, l'utilisateur reçoit automatiquement des droits d'administrateur iDRAC6. Cela est vrai même si le même utilisateur n'a pas de compte sur iDRAC6 ou si le compte n'a pas de droits d'administrateur.
- 1 Un utilisateur CMC pour lequel **Server Administrator** n'est pas défini sous **Privilèges utilisateur**, mais qui a le même compte sur iDRAC6, ouvrira automatiquement une session sur iDRAC6 à l'aide de la connexion directe. Une fois qu'il a ouvert une session sur l'interface Web iDRAC6, cet utilisateur reçoit les droits qui ont été créés pour le compte iDRAC6.

 **REMARQUE :** Dans ce contexte, *le même compte* signifie que l'utilisateur possède le même nom d'utilisateur et le même mot de passe pour CMC que pour iDRAC6. Un utilisateur ayant le même nom d'utilisateur, mais un mot de passe différent, n'est pas reconnu comme utilisateur valide.

- 1 Un utilisateur CMC pour lequel **Server Administrator** n'est pas défini sous **Privilèges utilisateur** ou qui n'a pas le même compte sur iDRAC6 n'ouvre pas automatiquement une session sur iDRAC6 à l'aide de la connexion directe. Cet utilisateur est dirigé vers l'écran d'ouverture de session iDRAC6 après avoir cliqué sur **Lancer l'interface utilisateur iDRAC6**.

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

 **REMARQUE :** Si le LAN réseau iDRAC6 est désactivé (LAN activé = non), la connexion directe n'est pas disponible.

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

Configuration de la mise en réseau pour iDRAC6

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6.

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

Pour activer ou désactiver Communications série sur le LAN :

- a. Cliquez sur **Communications série sur le LAN**.

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

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

Pour activer ou désactiver IPMI sur le LAN :

- a. Cliquez sur **Réseau**.

L'écran **Réseau** apparaît.

- b. Cliquez sur **Paramètres IPMI**.
- c. Cochez la case **Activer IPMI sur le LAN**. Vous pouvez également modifier les paramètres **Limite du niveau de privilège du canal** et **Clé de cryptage**.
- d. Cliquez sur **Appliquer**.

Pour activer ou désactiver DHCP :

- a. Cliquez sur **Réseau**.

L'écran **Réseau** apparaît.

- b. Cochez la case **Activer pour DHCP** dans la section **Paramètres IPv4** et la case **Activer pour l'autoconfiguration** dans la section **Paramètres IPv6** afin d'activer DHCP. Pour utiliser DHCP pour obtenir les adresses de serveur DNS, cochez la case **Utiliser DHCP pour obtenir des adresses de serveur DNS**.
- c. Cliquez sur **Appliquer**.

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

Visualisation des connexions de structure des cartes mezzanines FlexAddress

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

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

La fonctionnalité FlexAddress est configurée à l'aide de l'interface Web CMC. Pour plus d'informations sur la fonctionnalité FlexAddress et sa configuration, consultez le *Guide d'utilisation de Dell Chassis Management Controller* et le document *Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)*.

Lorsque la fonctionnalité FlexAddress a été activée et configurée pour le châssis, cliquez sur **Système** → onglet **Propriétés** → **WWN/MAC** pour afficher une liste des cartes mezzanines installées, les structures auxquelles elles sont connectées, le type de structure ainsi que les adresses MAC attribuées par le serveur ou le châssis à chaque port Ethernet intégré installé et à chaque port de carte mezzanine facultatif.

La colonne **Attribuée par le serveur** affiche les adresses WWN/MAC attribuées par le serveur qui sont incorporées au matériel du contrôleur Les adresses WWN/MAC affichant « - » indiquent que l'interface d'une structure spécifique n'a pas été installée.

La colonne **Attribuée par le châssis** affiche les adresses WWN/MAC attribuées par le châssis qui sont utilisées pour ce logement donné. Les adresses WWN/MAC affichant « - » indiquent que la fonctionnalité FlexAddress n'a pas été installée. Une coche dans les colonnes **Attribuée par le serveur** et **Attribuée par le châssis** indique les adresses actives.

FlexAddress MAC pour iDRAC6

La fonctionnalité FlexAddress remplace les adresses MAC attribuées par le serveur par les adresses MAC attribuées par le châssis et est désormais implémentée pour iDRAC6, ainsi que les LOM des lames, les cartes mezzanine et les modules d'E/S. La fonctionnalité FlexAddress de l'iDRAC6 prend en charge la préservation d'adresses MAC spécifiques à un logement pour les iDRAC6 d'un châssis. L'adresse MAC attribuée par le châssis est stockée dans la mémoire non volatile de CMC et est envoyée à iDRAC6 pendant son démarrage ou lorsque les paramètres de la page FlexAddress CMC sont modifiés.

Si CMC active les adresses MAC attribuées par le châssis, iDRAC6 affiche la valeur dans le champ Adresse MAC sur les écrans suivants :

- 1 **Système** → onglet **Propriétés** → **Détails du système** → Informations iDRAC6
- 1 **Système** → onglet **Propriétés** → WWN/MAC
- 1 **Système** → **Accès à distance** → iDRAC6 → onglet **Propriétés** → **Informations sur l'accès à distance** → **Paramètres réseau**
- 1 **Système** → **Accès à distance** → iDRAC6 → onglet **Réseau/Sécurité** → **Réseau** → **Paramètres de la carte d'interface réseau**

 **PRÉCAUTIONS** : Lorsque FlexAddress est activé, si vous passez d'une adresse MAC attribuée par le serveur à une adresse MAC attribuée par le châssis et vice-versa, l'adresse IP iDRAC6 change également.

 **REMARQUE** : Vous pouvez activer et désactiver la fonctionnalité FlexAddress uniquement via CMC. L'interface utilisateur de l'iDRAC6 rend uniquement compte de la condition. Toute session de console virtuelle ou de média virtuel existante est clôturée si le paramètre FlexAddress est modifié dans la page FlexAddress de CMC.

Activation de la fonctionnalité FlexAddress via la RACADM

Vous ne pouvez pas activer FlexAddress depuis iDRAC6. Activez FlexAddress aux niveaux du logement et de la structure depuis CMC.

- Depuis la console CMC, activez FlexAddress pour le serveur géré dans le logement avec la commande RACADM suivante :

```
racadm setflexaddr -i <n°_logement> 1, où <n°_logement> correspond au numéro de logement sur lequel activer FlexAddress.
```

- Ensuite, depuis la console CMC, activez FlexAddress au niveau de la structure en exécutant la commande RACADM suivante :

```
racadm setflexaddr -f <nom_de_la_structure> 1, où <nom_de_la_structure> correspond à A, B ou C.
```

- Pour activer FlexAddress pour tous les iDRAC6 du châssis, depuis la console CMC, exécutez la commande RACADM suivante :

```
racadm setflexaddr -f idrac 1
```

Consultez le *Guide de référence de l'administrateur de Dell Chassis Management Controller* pour plus d'informations sur les sous-commandes RACADM CMC.

Journal système distant

La fonctionnalité Journal système distant d'iDRAC6 vous permet d'écrire à distance le journal du RAC et le journal des événements système (SEL) sur un serveur de journaux système externe. Vous pouvez lire tous les journaux de l'ensemble de la batterie de serveurs à partir d'un journal central.

Le protocole Journal système distant ne nécessite aucune authentification de l'utilisateur. Quant aux journaux à saisir dans le serveur de journaux système distant, assurez-vous de la connectivité réseau entre iDRAC6 et le serveur de journaux système distant et que le serveur de journaux système distant s'exécute sur le même réseau qu'iDRAC6. Les entrées du Journal système distant sont transportées dans des paquets UDP envoyés au port de journal système du serveur de journaux système 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 RAC et le journal des événements système (SEL) de l'iDRAC6. Vous pouvez également modifier les paramètres du Journal système distant de l'iDRAC6 via le CMC.

Le journal système distant peut être activé via l'interface Web distante :

- Ouvrez une fenêtre d'un navigateur Web pris en charge.
- Ouvrez une session sur l'interface Web iDRAC6.
- Dans l'arborescence du système, sélectionnez **Système** → onglet **Configuration** → **Paramètres des journaux système distants**. L'écran **Paramètres des journaux système distants** s'affiche.

[Tableau 2-2](#) répertorie les paramètres des journaux système distants.

Tableau 2-2. Paramètres des journaux système distants

Attribut	Description
Journal système distant activé	Sélectionnez cette option pour activer la transmission et la saisie à distance du journal système sur le serveur spécifié. Lorsque le journal système est activé, de nouvelles entrées de journal sont envoyées à un ou à des serveurs de journaux système.
Serveur de journaux système 1-3	Saisissez l'adresse du serveur de journaux système distant afin de journaliser les messages iDRAC6 tels que le journal SEL et le journal du RAC. Les adresses du serveur de journaux système peuvent contenir des symboles alphanumériques, -, ., : et _.
Numéro de port	Saisissez le numéro de port du serveur de journaux système 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 Journal système distant diffèrent des niveaux de gravité standard du journal des événements système (SEL) IPMI. Toutes les entrées du journal système distant iDRAC6 sont ainsi rapportées dans le serveur de journaux système 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 journal système distant :

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogEnable [1/0] ; default is 0

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer1 <nom du serveur 1> ; default is blank

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer2 <servername2>; default is blank

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer3 <nom du serveur 3> ; default is blank

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPort <numéro de port> ; default is 514
```

Périphérique de démarrage initial

Cette fonctionnalité vous permet de sélectionner le périphérique de démarrage initial pour votre système et d'activer Démarrer une seule fois. 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. Si Démarrer une seule fois est activé, le système démarre depuis le périphérique sélectionné une seule fois et n'apparaît plus comme le périphérique de démarrage initial dans l'ordre de démarrage.

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.

[Tableau 2-3](#) répertorie les paramètres **Périphérique de démarrage initial**.

Tableau 2-3. 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.

Partage de fichiers distant

La fonctionnalité de partage de fichiers distant iDRAC6 vous permet de spécifier un fichier image ISO de CD/DVD sur un partage réseau et de le mettre à la disposition du système d'exploitation du serveur géré en tant que lecteur virtuel en le montant en tant que CD ou DVD à l'aide de NFS ou CIFS.

REMARQUE : Cette fonctionnalité fonctionne uniquement avec les adresses IPv4. Les adresses IPv6 ne sont actuellement pas prises en charge.

REMARQUE : Pour les distributions Linux, cette fonctionnalité peut nécessiter une commande mount manuelle en cas d'utilisation au niveau d'exécution init 3.

La syntaxe de la commande est la suivante :

mount /dev/OS_specific_device /<point de montage défini par l'utilisateur>

où <point de montage défini par l'utilisateur> correspond à un répertoire quelconque que vous choisissez d'utiliser pour le montage de la même façon qu'une commande mount quelconque.

Pour RHEL, le périphérique de CD (périphérique virtuel .iso) est /dev/scd0 et le périphérique de disquette (périphérique virtuel .img) est /dev/sdc.

Pour SLES, le périphérique de CD est /dev/sr0 et le périphérique de disquette est /dev/sdc.

Pour vous assurer que le bon périphérique est utilisé (pour SLES ou pour RHEL), lorsque vous connectez le périphérique virtuel, vous devez

immédiatement exécuter la commande sur le SE Linux :

```
tail /var/log/messages | grep SCSI
```

Ceci affichera le texte qui identifie le périphérique (par exemple, périphérique SCSI sdc).

Cette procédure s'applique également au média virtuel lorsque vous utilisez les distributions Linux au niveau d'exécution init 3. Par défaut, le média virtuel n'est pas monté automatiquement au niveau d'exécution init 3.

Le chemin de l'image partagée CIFS doit être au format :

```
//<adresse ip ou nom de domaine>/<partage_nom>/<cheminversimage>
```

Le chemin de l'image partagée via NFS doit être au format :

```
<adresse ip>:/<cheminversimage>
```

Si un nom d'utilisateur contient un nom de domaine, le nom d'utilisateur doit alors être saisi au format <nom d'utilisateur>@<domaine>. Par exemple, `user1@dell.com` est un nom d'utilisateur valide, à l'inverse de `dell\user1`.

Un nom de fichier qui se termine par l'extension IMG est redirigé en tant que disquette virtuelle et un nom de fichier qui se termine par l'extension ISO est redirigé en tant que CD-ROM virtuel. Le partage de fichiers distant prend uniquement en charge les formats de fichier image .IMG et .ISO.

La fonctionnalité RFS utilise l'implémentation de média virtuel sous-jacente dans iDRAC6. Vous devez posséder des privilèges Média virtuel pour procéder au montage de RFS. Si un lecteur virtuel est déjà utilisé par le média virtuel, le lecteur ne pourra alors pas être monté en tant que RFS et vice versa. Pour que RFS fonctionne, le média virtuel dans iDRAC6 doit alors être en mode *Connecter* ou *Connecter automatiquement*.

L'état de la connexion de RFS est disponible dans le journal iDRAC6. Une fois connecté, un lecteur virtuel monté en tant que RFS ne se déconnecte pas, même si vous fermez la session sur iDRAC6. La connexion RFS est fermée si iDRAC6 est réinitialisé ou si la connexion réseau est coupée. Les options de l'interface utilisateur et de la ligne de commande sont également disponibles dans CMC et iDRAC6 afin de fermer la connexion RFS. La connexion RFS à partir de CMC remplace toujours un montage RFS existant dans iDRAC6.

 **REMARQUE :** La fonctionnalité vFlash d'iDRAC6 et RFS n'ont aucun lien entre eux.

Pour activer le partage de fichiers distant via l'interface Web iDRAC6, procédez comme suit :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Sélectionnez **Système** → onglet **Partage de fichiers distant**.

L'écran **Partage de fichiers distant** apparaît.

[Tableau 2-4](#) répertorie les paramètres du partage de fichiers distant.

Tableau 2-4. Paramètres du serveur de fichiers à distance

Attribut	Description
Nom d'utilisateur	Nom d'utilisateur pour se connecter au système de fichiers NFS/CIFS.
Mot de passe	Mot de passe pour se connecter au système de fichiers NFS/CIFS.
Chemin d'accès du fichier image	Chemin d'accès du fichier à partager via le partage de fichiers distant.
Condition	Connecté : le fichier est partagé. Non connecté : le fichier n'est pas partagé. Connexion en cours... : connexion au partage en cours

Cliquez sur **Connecter** afin d'établir une connexion de partage de fichiers. Le bouton **Connecter** est désactivé après l'établissement de la connexion.

 **REMARQUE :** Même si vous avez configuré le partage de fichiers distant, l'interface utilisateur n'affiche pas cette information pour des raisons de sécurité.

Pour le partage de fichiers à distant, la commande RACADM distante est

```
racadm remoteimage.
```

```
racadm remoteimage <options>
```

Les options sont les suivantes :

-c ; connecter image

-d ; déconnecter image

-u <nom d'utilisateur> ; nom d'utilisateur permettant d'accéder au partage réseau

-p <mot de passe> ; mot de passe permettant d'accéder au partage réseau

-l <emplacement_de_l'image> ; emplacement de l'image sur le partage réseau ; mettez des guillemets autour de l'emplacement

-s ; affiche la condition actuelle

 **PRÉCAUTIONS :** Tous les caractères, caractères alphanumériques et spéciaux compris, peuvent faire partie du nom d'utilisateur, du mot de passe et de emplacement_de_l'image, à l'exception des caractères suivants : ' (guillemets simples), " (guillemets doubles), (virgule), < (inférieur à) et > (supérieur à). Lorsque vous utilisez un partage de fichiers distant, les caractères susmentionnés ne peuvent pas faire partie du nom d'utilisateur, du mot de passe et de emplacement_de_l'image.

Module SD interne double

Le module SD interne double (IDSMD) est disponible uniquement sur les plateformes concernées. IDSMD assure la redondance sur la carte SD de l'hyperviseur en utilisant une autre carte SD qui met en miroir le contenu de la première carte SD. La carte SD vFlash iDRAC6, avec la deuxième carte SD, peut être définie sur IDSMD en définissant l'option **Redondance** sur **Mode Miroir** dans l'écran **Périphériques intégrés** de la configuration du BIOS du système. Lorsque la fonctionnalité IDSMD est activée, la fonctionnalité vFlash de la carte SD vFlash iDRAC6 n'est pas disponible et cette carte est définie comme la carte SD secondaire dans IDSMD. Pour plus d'informations sur les options du BIOS pour IDSMD, consultez le *Manuel du propriétaire* disponible sur le site Web du support

de Dell à l'adresse support.dell.com/manuals.

REMARQUE : Dans la configuration du BIOS, dans l'écran **Périphériques intégrés**, l'option **Port USB interne** doit être définie sur **Activé**. Si elle est définie sur **Désactivé**, IDSDM ne sera pas visible par le système en tant que périphérique de démarrage.

L'une des deux cartes SD peut être la carte maîtresse. Par exemple, si deux nouvelles cartes SD sont installées dans IDSDM, SD1 deviendra la carte active ou maîtresse. SD2 sera la carte de sauvegarde et toutes les écritures IDSDM du système de fichiers se feront sur les deux cartes, mais les lectures auront lieu uniquement depuis SD1. À tout moment, si SD1 échoue ou est retirée, SD2 devient automatiquement la carte active (maîtresse).

Tableau 2-5. Condition IDSDM

IDSDM : mode Miroir	Carte SD	Carte SD vFlash
Activé	Active (carte SD2)	vFlash inactif, devient la carte SD2 active
Désactivé	Active (carte SD2)	Seul vFlash est actif

Vous pouvez utiliser iDRAC pour afficher la condition, l'intégrité et la disponibilité d'IDSDM.

La condition de redondance de la carte SD et les événements de panne sont consignés dans le journal SEL et affichés sur l'écran LCD, et des alertes PET sont générées si les alertes sont activées.

Affichage de la condition du module SD interne double via l'interface utilisateur

- Ouvrez une session sur l'interface utilisateur Web iDRAC.
- Dans l'arborescence du **système**, cliquez sur **Média flash amovible**. La page **Média vFlash amovible** s'affiche. Cette page présente les deux sections suivantes :
 - Module SD interne double** : affiché uniquement si IDSDM est en mode redondant. La **Condition de redondance** est affichée sous la forme **Total**. Si cette section n'est pas présente, la carte est alors en mode non redondant. Les indications valides de la **Condition de redondance** sont :
 - Total** : les cartes SD 1 et 2 fonctionnent correctement.
 - Perdu** : une ou les deux cartes SD ne fonctionnent pas correctement.
 - Condition du module SD interne** : affiche l'état des cartes SD1 et SD2 avec les informations suivantes :
 - Condition :
 -  : indique que la carte est correcte.
 -  : indique que la carte est hors ligne ou protégée contre l'écriture.
 -  : indique qu'une alerte a été émise.
 - Emplacement : emplacement des cartes SD.
 - Condition en ligne : les cartes SD1 et SD2 peuvent se trouver dans un des états indiqués dans [Tableau 2-6](#).

Tableau 2-6. États des cartes SD1 et SD2

État	Description
Démarrage	Le contrôle est en cours de mise sous tension.
Actif	La carte reçoit toutes les écritures SD et est utilisée pour les lectures SD.
Veille	La carte est la carte secondaire. Elle reçoit une copie de toutes les écritures SD.
Échec	Une erreur est signalée lors d'une lecture ou d'une écriture de carte SD.
Absent	La carte SD n'est pas détectée.
Hors ligne	Au démarrage, la signature CID de la carte est différente de la valeur de stockage NV ou la carte constitue la destination d'une opération de copie en cours.
Protégé contre l'écriture	La carte est protégée contre l'écriture par le loquet physique situé sur la carte SD. IDSDM ne peut pas utiliser une carte protégée contre l'écriture.

Mise à jour du micrologiciel iDRAC6

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

- Interface Web iDRAC6
- CLI RACADM
- Progiciel de mise à jour Dell (pour Linux ou Microsoft Windows)

- 1 Utilitaire de mise à jour du micrologiciel iDRAC6 DOS
- 1 Interface Web CMC

Téléchargement du micrologiciel ou du progiciel de mise à jour

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

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

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

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

Exécution de la mise à jour du micrologiciel

 **REMARQUE :** Lorsque la mise à jour du micrologiciel iDRAC6 commence, toutes les sessions iDRAC6 existantes sont déconnectées et les nouvelles sessions ne sont pas autorisées tant que le processus de mise à jour n'est pas terminé.

 **REMARQUE :** Les ventilateurs du châssis s'exécutent à 100 % lors de la mise à jour du micrologiciel iDRAC6. Lorsque la mise à jour est terminée, la régulation de la vitesse normale du ventilateur reprend. Il s'agit d'un comportement normal visant à protéger le serveur contre toute surchauffe durant le laps de temps au cours duquel il ne peut pas envoyer d'informations de capteur à CMC.

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

Lorsque vous utilisez l'interface Web iDRAC6 ou l'interface Web CMC, placez l'image binaire du micrologiciel sur un disque accessible à la station de gestion à partir de laquelle vous exécutez l'interface Web. Consultez [Mise à jour du micrologiciel iDRAC6](#).

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

Vous pouvez utiliser l'interface Web CMC ou la RACADM CMC pour mettre à jour le micrologiciel iDRAC6. Cette fonctionnalité est disponible lorsque le micrologiciel iDRAC6 est en mode Normal ou lorsqu'il est corrompu. Consultez [Mise à jour du micrologiciel iDRAC6 avec CMC](#).

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

 **REMARQUE :** Si vous rétablissez une version antérieure du micrologiciel iDRAC6, supprimez le plug-in ActiveX Internet Explorer existant sur n'importe quelle station de gestion Windows afin que le micrologiciel puisse installer une version compatible du plug-in ActiveX.

Vérification de la signature numérique pour les DUP Linux.

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

Si vous ne l'avez pas encore installé sur votre système, vous devez installer le dispositif de protection GPG (Gnu Privacy Guard) pour vérifier une signature numérique.

Pour utiliser la procédure de vérification standard, suivez les étapes suivantes :

1. Téléchargez la clé GnuPG publique Dell Linux en naviguant vers lists.us.dell.com et en cliquant sur le lien **Dell Public GPG key**. Enregistrez le fichier sur votre système local. Le nom par défaut est **linux- security- publickey.txt**.
2. Importez la clé publique dans votre base de données de confiance gpg en exécutant la commande suivante :

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

 **REMARQUE :** Vous devez avoir votre clé privée pour terminer le processus.

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

a. Entrez la commande suivante :

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

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

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

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

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

```
Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from different sources, etc.)
(Veuillez préciser à quel point vous faites confiance à cet utilisateur pour vérifier correctement les clés des autres utilisateurs (en examinant les passeports, en vérifiant les empreintes à partir de différentes sources, etc.))
```

```
1 = I don't know or won't say (Je ne sais pas ou ne souhaite pas me prononcer)
2 = I do NOT trust (Je NE fais PAS confiance)
3 = I trust marginally (Je fais un peu confiance)
4 = I trust fully (Je fais entièrement confiance)
5 = I trust ultimately (Je fais définitivement confiance)
m = back to the main menu (retour au menu principal)
```

Your decision? (Votre décision ?)

d. Tapez `5`, puis appuyez sur `<Entrée>`. L'invite suivante apparaît :

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

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

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

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

4. Procurez-vous le progiciel dont vous avez besoin (par exemple, le progiciel DUP Linux ou l'archive à extraction automatique) et son fichier de signature associé sur le site Web du support de Dell à l'adresse support.dell.com/support/downloads.



REMARQUE : Chaque progiciel de mise à jour Linux dispose d'un fichier de signature distinct, qui s'affiche sur la même page Web que le progiciel de mise à jour. Il vous faut le progiciel de mise à jour et le fichier de signature qui lui est associé pour la vérification. Par défaut, le fichier de signature porte le même nom que le fichier DUP avec une extension `.sign`. Par exemple, l'image du micrologiciel iDRAC6 est associée à un fichier `.sign` (`IDRAC_FRMW_LX_2.2.BIN.sign`), qui est inclus dans l'archive à extraction automatique avec l'image du micrologiciel (`IDRAC_FRMW_LX_2.2.BIN`). Pour télécharger les fichiers, cliquez avec le bouton droit de la souris sur le lien **Télécharger** et utilisez l'option **Enregistrer la cible en tant que**.

5. Vérifiez le progiciel de mise à jour :

```
gpg --verify <Nom de fichier de la signature du progiciel DUP Linux> <Nom de fichier du progiciel DUP Linux>
```

L'exemple suivant illustre les étapes à suivre pour vérifier un progiciel de mise à jour de Dell PowerEdge M610 iDRAC6 :

1. Téléchargez les deux fichiers suivants à partir de support.dell.com :

```
1 IDRAC_FRMW_LX_2.2.BIN.sign
1 IDRAC_FRMW_LX_2.2.BIN
```

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

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

Le message suivant apparaît :

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

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

a. Entrez la commande suivante :

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

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

```
fpr
trust
```

c. Entrez `5`, puis appuyez sur `<Entrée>` pour choisir Je fais définitivement confiance dans le menu.

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

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

Cette opération termine la validation de la clé publique Dell.

4. Vérifiez la signature numérique du progiciel Dell PowerEdge M610 iDRAC6 en exécutant la commande suivante :

```
gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign IDRAC_FRMW_LX_2.2.BIN
```

Le message suivant apparaît :

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

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

```
gpg: WARNING: This key is not certified with a trusted signature! (gpg : AVERTISSEMENT : Cette clé n'est pas certifiée avec une signature de confiance !)
gpg: There is no indication that the signature belongs to the owner. (gpg : Il n'y a aucune indication que la signature appartienne au propriétaire).
Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D (Empreinte de clé primaire : 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D)
```

Utilisation de l'interface Web iDRAC6

 **REMARQUE :** Si la progression de la mise à jour du micrologiciel iDRAC6 est interrompue avant qu'elle ne se termine, le micrologiciel iDRAC6 peut être corrompu. Dans ces cas-là, vous pouvez récupérer iDRAC6 à l'aide de l'interface Web CMC.

 **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 rétablir les paramètres d'usine de la configuration iDRAC6. Si vous rétablissez les paramètres d'usine de la configuration, l'accès réseau externe sera désactivé une fois la mise à jour terminée. Vous devez activer et configurer le réseau à l'aide de l'utilitaire de configuration iDRAC6.

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

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

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

4. Dans la section **Téléverser**, cliquez sur **Parcourir pour localiser** l'image de micrologiciel que vous avez téléchargée. Vous pouvez également entrer le chemin dans le champ de texte. Par exemple :

```
C:\Updates\V2.2\<nom_de_l' image>.
```

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

5. Cliquez sur **Téléverser**.

Le fichier se télécharge sur iDRAC6. Cette opération peut prendre plusieurs minutes.

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

À la fin du téléversement, l'écran **Téléverser (étape 2 sur 3)** s'affiche.

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

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

6. Par défaut, l'option **Préserver la configuration** est activée (cochée) pour préserver les paramètres actuels sur iDRAC6 après une mise à niveau. Si vous ne voulez pas que les paramètres soient préservés, décochez la case **Préserver la configuration**.
7. Cliquez sur **Démarrer la mise à jour** pour démarrer le processus de mise à niveau. N'interrompez pas le processus de mise à niveau.
8. La fenêtre **Téléverser (étape 3 sur 3)** affiche la condition de la mise à jour. La progression de l'opération de mise à niveau de micrologiciel, mesurée en pourcentage, apparaît dans la colonne **Progression**.
9. Une fois la mise à jour du micrologiciel terminée, la fenêtre **Téléverser (étape 3 sur 3)** s'actualise avec le résultat et iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC6 avec une nouvelle fenêtre de navigateur.

Mise à jour du micrologiciel iDRAC6 via la RACADM

Vous pouvez mettre à jour le micrologiciel iDRAC6 à l'aide de la RACADM distante.

1. Téléchargez sur le système géré l'image de micrologiciel iDRAC6 sur le site Web du support de Dell à l'adresse support.dell.com.

Par exemple :

```
C:\downloads\firmimg.imc
```

2. Exécutez la commande RACADM suivante :

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.imc* est stocké.

Utilisation de l'utilitaire de mise à jour DOS

Pour mettre à jour le micrologiciel iDRAC6 à l'aide de l'utilitaire de mise à jour DOS, démarrez le serveur géré sur DOS et exécutez la commande `idrac16d`. La syntaxe de la commande est la suivante :

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

Lorsqu'elle est exécutée sans option, la commande `idrac16d` met à jour le micrologiciel iDRAC6 à l'aide du fichier image du micrologiciel `firmimg.imc` dans le répertoire actuel.

Les options sont les suivantes :

- 1 `-f` : force la mise à jour. L'option `-f` peut être utilisée pour *rétrograder* le micrologiciel à une image antérieure.
- 1 `-i=<nom de fichier>` : spécifie le nom de fichier de l'image du micrologiciel. Cette option est requise si le nom de fichier par défaut `firmimg.imc` du micrologiciel a été modifié.
- 1 `-l=<fichier journal>` : consigne le résultat de l'activité de mise à jour. Cette option est utilisée pour le débogage.

 **REMARQUE :** Si vous entrez des arguments incorrects pour la commande `idrac16d` ou indiquez l'option `-h`, il est possible que vous remarquiez une option supplémentaire, `-nopresconfig`, dans le résultat d'utilisation. Cette option est utilisée pour mettre à jour le micrologiciel sans conserver les informations sur la configuration. Il est recommandé de **ne pas** utiliser cette option, car elle *supprime* toutes vos informations existantes sur la configuration iDRAC6 telles que les adresses IP, les utilisateurs et les mots de passe.

Mise à jour du progiciel de réparation de l'USC

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

Configuration d'iDRAC6 pour l'utiliser avec IT Assistant

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

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

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

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

Lorsque l'écran **Utilitaire de configuration** de l'iDRAC6 apparaît, utilisez les touches fléchées pour faire défiler vers le bas.

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

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

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

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

 **REMARQUE :** Vous pouvez également utiliser Dell Management Console, l'application de gestion de systèmes « un à plusieurs » de nouvelle génération, pour activer la découverte et la surveillance. Pour plus d'informations, consultez le *Guide d'utilisation de Dell Management Console* disponible sur le site du support de Dell à l'adresse support.dell.com/manuals.

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

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

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6 en utilisant un nom d'ouverture de session et un mot de passe possédant des droits d'administrateur.
3. Dans l'arborescence du système, sélectionnez **Système** → **Accès à distance** → **iDRAC6**.
4. Cliquez sur l'onglet **Réseau/Sécurité**.
L'écran **Réseau** apparaît.
5. Cliquez sur **Paramètres IPMI**.
6. Vérifiez que la case **Activer IPMI sur le LAN** est sélectionnée (cochée).
7. Sélectionnez **Administrateur** dans le menu déroulant **Limite du niveau de privilège du canal**.
8. Saisissez **la clé de cryptage RMCP+** de votre site, si elle est utilisée.
9. Cliquez sur **Appliquer** si vous avez apporté des modifications dans cet écran.
10. Dans l'arborescence du système, sélectionnez **Système**.
11. Cliquez sur l'onglet **Gestion des alertes**, puis sur **Événements sur plateforme**.
L'écran **Événements sur plateforme** apparaît, affichant une liste des événements pour lesquels vous pouvez configurer iDRAC6 pour qu'il génère des alertes par e-mail.
12. Activez les alertes par e-mail pour un ou plusieurs événements en cochant la case dans la colonne **Générer une alerte**.
13. Cliquez sur **Appliquer** si vous avez apporté des modifications dans cet écran.
14. Cliquez sur **Paramètres des interruptions**.
L'écran **Paramètres des interruptions** apparaît.
15. Dans le premier champ **Adresse IP de destination** disponible dans la section **Liste des destinations IPv4**, cochez la case **Activé**, puis entrez l'adresse IP de votre station de gestion.
16. Cliquez sur **Appliquer** si vous avez apporté des modifications dans cet écran.

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

Dell vous recommande vivement, à des fins de sécurité, de créer un utilisateur séparé pour les commandes IPMI avec son propre nom d'utilisateur, ses propres privilèges IPMI sur le LAN et son propre mot de passe :

1. Dans l'arborescence du système, sélectionnez **Système** → **Accès à distance** → **iDRAC6**.

2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Utilisateurs**.

L'écran **Utilisateurs** apparaît, affichant une liste de tous les utilisateurs (définis ou non définis).

3. Cliquez sur la **Réf. utilisateur** d'un utilisateur non défini.

L'écran Configuration utilisateur pour la réf. utilisateur sélectionnée apparaît.

4. Cochez la case **Activer l'utilisateur**, puis entrez le nom et le mot de passe de l'utilisateur.

5. Dans la section **Privilèges LAN IPMI**, vérifiez que **Maximum de privilèges utilisateur accordés sur le LAN** est défini sur **Administrateur**.

6. Définissez les autres privilèges utilisateur selon les besoins.

7. Cliquez sur **Appliquer** pour enregistrer les nouveaux paramètres Utilisateur.

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

Lorsque la découverte est terminée, les périphériques iDRAC6 s'affichent dans la catégorie **Serveurs** de l'écran **Détails des périphériques ITA** et les informations iDRAC6 peuvent être affichées en cliquant sur le nom d'iDRAC6. Ceci diffère des systèmes DRAC 5 pour lesquels la carte de gestion apparaît dans le groupe RAC.

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

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

 **REMARQUE :** Vous pouvez également utiliser Dell Management Console, l'application de gestion de systèmes « un à plusieurs » de nouvelle génération, pour afficher la condition et les événements d'iDRAC6. Pour plus d'informations, consultez le *Guide d'utilisation de Dell Management Console* sur le site du support de Dell à l'adresse support.dell.com/manuals.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration de la station de gestion

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Étapes de configuration de la station de gestion](#)
- [Impératifs de réseau de la station de gestion](#)
- [Configuration d'un navigateur Web pris en charge](#)
- [Installation du logiciel iDRAC6 sur la station de gestion](#)
- [Installation d'un environnement d'exécution Java \(JRE\)](#)
- [Installation de clients Telnet ou SSH](#)
- [Installation d'un serveur TFTP](#)
- [Installation de Dell OpenManage IT Assistant](#)
- [Installation de Dell Management Console](#)

Une station de gestion est un ordinateur servant à surveiller et à gérer les serveurs Dell PowerEdge ainsi que les autres modules du châssis. Cette section décrit les tâches d'installation et de configuration logicielles permettant de configurer une station de gestion afin qu'elle puisse fonctionner avec iDRAC6 Enterprise. Avant de commencer à configurer iDRAC6, suivez les procédures de cette section afin de vous assurer que vous avez installé et configuré les outils dont vous aurez besoin.

Étapes de configuration de la station de gestion

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

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

Impératifs de réseau de la station de gestion

Pour accéder à iDRAC6, la station de gestion doit se trouver sur le même réseau que le port de connexion RJ45 CMC appelé « GB1 ». Il est possible d'isoler le réseau CMC du réseau sur lequel se trouve le serveur géré, de sorte que votre station de gestion puisse disposer d'un accès LAN à iDRAC6, mais non au serveur géré.

Grâce à la fonctionnalité Console virtuelle d'iDRAC6 (consultez [Configuration et utilisation des communications série sur le LAN](#)), vous pouvez accéder à la console du serveur géré, même si vous ne disposez pas d'un accès réseau aux ports du serveur. Vous pouvez également exécuter plusieurs fonctions de gestion sur le serveur géré, comme le redémarrage de l'ordinateur et l'utilisation des services iDRAC6. Pour accéder aux services réseau et d'application hébergés sur le serveur géré, il vous faudra peut-être cependant un NIC supplémentaire sur le serveur géré.

Configuration d'un navigateur Web pris en charge

Les sections suivantes fournissent des instructions pour la configuration des navigateurs Web pris en charge afin de les utiliser avec l'interface Web iDRAC6.

Ouverture de votre navigateur Web

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

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

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

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

Pour configurer le navigateur Web Internet Explorer pour accéder à un serveur proxy, suivez les étapes suivantes :

1. Ouvrez une fenêtre de navigateur Web.
2. Cliquez sur **Outils**, puis sur **Options Internet**.
La fenêtre **Options Internet** apparaît.
3. Sélectionnez **Outils**→ **Options Internet**→ **Sécurité**→ **Réseau local**.
4. Cliquez sur **Personnaliser le niveau**.
5. Sélectionnez **Moyen-bas** dans le menu déroulant et cliquez sur **Réinitialiser**. Cliquez sur **OK** pour confirmer. Vous devez accéder à nouveau à la boîte de dialogue **Personnaliser le niveau** en cliquant sur le bouton correspondant.
6. Ensuite, faites défiler vers le bas vers la section intitulée **Contrôles ActiveX et plug-ins** et vérifiez chaque paramètre, car les différentes versions d'IE comportent des paramètres différents dans l'état **Moyen-bas** :

- 1 Demander confirmation pour les contrôles ActiveX : Activé
- 1 Comportements de fichiers binaires et des scripts : Activé
- 1 Télécharger les contrôles ActiveX signés : Demander
- 1 Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés pour l'écriture de scripts : Demander
- 1 Exécuter les contrôles ActiveX et les plug-ins : Activé
- 1 Contrôles ActiveX reconnus sûrs pour l'écriture de scripts : Activé

Dans la section relative aux **Téléchargements** :

- 1 Demander confirmation pour les téléchargements de fichiers : Activé
- 1 Téléchargement de fichiers : Activé
- 1 Téléchargement de polices : Activé

Dans la section **Divers** :

- 1 Autoriser l'actualisation des métafichiers : Activé
- 1 Autoriser les scripts de contrôle du navigateur Web Internet Explorer : Activé
- 1 Autoriser les fenêtres initiées par des scripts sans contraintes de taille ou de position : Activé
- 1 Ne pas demander la sélection d'un certificat client lorsqu'il n'existe qu'un seul certificat ou aucun : Activé
- 1 Lancement des programmes et des fichiers dans un IFRAME : Activé
- 1 Ouvrir les fichiers en fonction de leur contenu, pas de leur extension de fichier : Activé
- 1 Permissions du canal du logiciel : Sécurité basse
- 1 Soumettre les données de formulaire non codées : Activé
- 1 Utiliser le bloqueur de fenêtres publicitaires : Désactivé

Dans la section **Script** :

- 1 Script actif : Activé
- 1 Autoriser les opérations de collage via un script : Activé
- 1 Script des applets Java : Activé

- 1 Sélectionnez **Outils**→ **Options Internet**→ **Avancé**.

- 1 Assurez-vous que les éléments suivants sont cochés ou décochés :

Dans la section **Navigaton** :

- 1 Toujours envoyer des URL en tant que UTF-8 : **coché**
- 1 Désactiver le débogage des scripts (Internet Explorer) : **coché**
- 1 Désactiver le débogage des scripts (autres applications) : **coché**
- 1 Afficher une notification de chaque erreur de script : **décoché**
- 1 Activer l'installation sur demande (autres applications) : **coché**
- 1 Autoriser les transitions entre les pages : **coché**
- 1 Activer les extensions tierce partie du navigateur : **coché**
- 1 Réutiliser les fenêtres pour lancer des raccourcis : **décoché**

Dans la section **Paramètres HTTP 1.1** :

- Utiliser HTTP 1.1 : coché
- Utiliser HTTP 1.1 avec une connexion par proxy : coché

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

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

Dans la section **Multimédia** :

- Autoriser le redimensionnement automatique de l'image : coché
- Lire les animations dans les pages Web : coché
- Lire les sons dans les pages Web : coché
- Afficher les images : coché

Dans la section **Sécurité** :

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

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

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

Ajout d'iDRAC6 à la liste des domaines de confiance

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

Sur certains systèmes d'exploitation, il est possible qu'Internet Explorer (IE) 8 ne vous invite pas à ajouter l'adresse IP iDRAC6 à la liste des domaines de confiance si l'adresse IP ne figure pas dans la liste.

 **REMARQUE** : Lorsque vous vous connectez à l'interface Web iDRAC avec un certificat en lequel le navigateur n'a pas confiance, l'avertissement lié au certificat du navigateur peut apparaître une deuxième fois après que vous avez accusé réception du premier avertissement. Ce comportement attendu permet de garantir la sécurité.

Pour ajouter l'adresse IP iDRAC6 à la liste des domaines de confiance dans IE8, procédez comme suit :

1. Sélectionnez **Outils** → **Options Internet** → **Sécurité** → **Sites de confiance** → **Sites**.
2. Saisissez l'adresse IP iDRAC6 dans **Ajouter ce site Web à la zone**.
3. Cliquez sur **Ajouter**.
4. Cliquez sur **OK**.
5. Cliquez sur **Fermer**.

6. Cliquez sur **OK** puis actualisez votre navigateur.

Lorsque vous lancez la console virtuelle pour la première fois via IEB avec un plug-in Active-X, le message "Certificate Error: Navigation Blocked" (« Erreur de certificat : navigation bloquée ») peut s'afficher.

1. Cliquez sur **Continuer vers ce site Web**.
2. Cliquez sur **Installer** pour installer les contrôles Active-X dans la fenêtre **Avertissement de sécurité**.

La session de console virtuelle est lancée.

Affichage des versions localisées de l'interface Web

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

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

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

L'interface Web iDRAC6 est conçue pour fonctionner avec des claviers localisés pour les variantes de langue spécifiques répertoriées ci-dessus. Certaines fonctionnalités de l'interface Web iDRAC6, comme la console virtuelle, peuvent nécessiter des étapes supplémentaires afin de pouvoir accéder à certaines fonctions/lettres. Pour plus de détails sur l'utilisation des claviers localisés dans ces situations, consultez [Utilisation de Video Viewer](#). L'utilisation d'autres claviers n'est pas prise en charge et peut entraîner des problèmes inattendus.



REMARQUE : Consultez la documentation de votre navigateur Web pour obtenir des informations sur le mode de configuration ou d'installation de différentes langues et afficher des versions localisées de l'interface Web iDRAC6.

Configuration des paramètres régionaux sous Linux

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

Pour définir le jeu de caractères sur un client Linux avec une interface utilisateur en chinois simplifié :

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

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. Si les valeurs incluent zh_CN.UTF-8, aucune modification n'est requise. Si les valeurs n'incluent pas zh_CN.UTF-8, passez à l'étape 4.
4. Modifiez le fichier `/etc/sysconfig/i18n` à l'aide d'un éditeur de texte.
5. Dans le fichier, appliquez les modifications suivantes :

Entrée actuelle :

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

Entrée mise à jour :

```
LANG="zh_CN.UTF-8"
```

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

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

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

Désactivation de la fonctionnalité de liste blanche dans Firefox

Firefox intègre une fonctionnalité de sécurité de « liste blanche » qui requiert une autorisation utilisateur pour installer des plug-ins pour chaque site distinct hébergeant un plug-in. Si elle est activée, la fonctionnalité de liste blanche vous oblige à installer un visualiseur de console virtuelle pour chaque iDRAC6 visité, même si les versions de visualiseur sont identiques.

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

1. Ouvrez une fenêtre de navigateur Web Firefox.
2. Dans le champ d'adresse, entrez `about:config` et appuyez sur <Entrée>.
3. Dans la colonne **Nom de la préférence**, recherchez et double-cliquez sur `xpinstall.whitelist.required`.

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

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

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

Installation du logiciel iDRAC6 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 :

- 1 Racine du DVD : contient Dell Systems Build and Update Utility, qui fournit des informations de configuration du serveur et d'installation du système
- 1 SYSMGMT : contient les produits Systems Management Software, dont Dell OpenManage Server Administrator

Installation et désinstallation de la RACADM sur une station de gestion

Pour utiliser les fonctions de la RACADM distante, installez la RACADM sur une station de gestion. Consultez le *Guide d'installation de Dell OpenManage Management Station Software* disponible à l'adresse support.dell.com/manuals pour des informations sur l'installation des outils DRAC sur une station de gestion fonctionnant sous un système d'exploitation Microsoft Windows.

Installation et désinstallation de la RACADM sous Linux

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.

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

```
rpm -e <nom_du_progiciel_racadm>
```

où `<nom_du_progiciel_racadm>` est le paquetage RPM qui a été utilisé pour installer le logiciel iDRAC6.

Par exemple, si le nom du paquetage RPM est `srvadmin-racadm5`, tapez :

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

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

 **REMARQUE :** Si vous utilisez Internet Explorer, un contrôle ActiveX est fourni pour le visualiseur de console virtuelle. Vous pouvez également utiliser le visualiseur de console virtuelle Java avec Firefox si vous installez un JRE et configurez le visualiseur de console virtuelle dans l'interface Web iDRAC6 avant de lancer le visualiseur. Consultez la section [Configuration de la console virtuelle et du média virtuel dans l'interface Web iDRAC6](#) pour plus d'informations.

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

Si vous utilisez le navigateur Firefox, vous devez installer un JRE (ou un kit de développement Java [JDK]) pour pouvoir utiliser la fonctionnalité Console virtuelle. Le visualiseur de console virtuelle est une application Java téléchargée sur la station de gestion à partir de l'interface Web iDRAC6, puis lancée avec Java Web Start sur la station de gestion.

Accédez au site java.sun.com pour installer un JRE ou JDK. La version 1.6 (Java 6.0) ou ultérieure est recommandée.

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

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

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

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

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

Installation de clients Telnet ou SSH

Par défaut, le service Telnet iDRAC6 est désactivé et le service SSH est activé. Étant donné que Telnet est un protocole non sécurisé, vous devez uniquement l'utiliser si vous ne pouvez pas installer un client SSH ou si votre connexion réseau est sécurisée.

 **REMARQUE :** iDRAC6 prend en charge jusqu'à 4 sessions Telnet et 4 sessions SSH simultanément.

Telnet avec iDRAC6

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

Configuration de la touche Retour pour les sessions 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 Telnet Microsoft pour qu'ils utilisent la touche <Retour>, suivez les étapes suivantes :

1. Ouvrez une fenêtre d'invite de commande (si nécessaire).
2. Si vous n'exécutez pas de session Telnet, entrez :

```
telnet
```

Si vous exécutez une session Telnet, appuyez sur <Ctrl><J>.

3. À l'invite, entrez :

```
set bsasdel
```

Le message suivant apparaît :

```
Backspace will be sent as delete. (Retour arrière sera envoyé en tant que supprimer).
```

Pour configurer une session Telnet Linux pour pouvoir utiliser la touche <Retour>, suivez les étapes suivantes :

1. Ouvrez un environnement et entrez :

```
stty erase ^h
```

2. À l'invite, entrez :

telnet

SSH avec iDRAC6

Secure Shell (SSH) est une connexion de ligne de commande ayant les mêmes fonctions qu'une session Telnet, mais intégrant la négociation de session et le cryptage pour améliorer la sécurité. iDRAC6 prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé par défaut sur iDRAC6.

Vous pouvez utiliser des programmes gratuits tels que PuTTY ou OpenSSH sur une station de gestion pour vous connecter à l'iDRAC6 du serveur géré. Lorsqu'une erreur se produit lors de la procédure d'ouverture de session, le client SSH publie un message d'erreur. Le texte du message dépend du client et n'est pas contrôlé par iDRAC6.

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

iDRAC6 prend en charge jusqu'à 4 sessions Telnet et 4 sessions SSH simultanément. Cependant, uniquement une de ces 8 sessions potentielles peut utiliser SM-CLP. En d'autres termes, iDRAC6 prend en charge uniquement une session SM-CLP à la fois. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout`, comme décrit dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

La mise en œuvre SSH iDRAC6 prend en charge plusieurs schémas de cryptographie, comme illustré dans [Tableau 3-1](#).

 **REMARQUE :** SSHv1 n'est pas pris en charge.

Tableau 3-1. Schémas de cryptographie

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

Installation d'un serveur TFTP

 **REMARQUE :** Si vous utilisez uniquement l'interface Web iDRAC6 pour transférer des certificats SSL et téléverser un nouveau micrologiciel iDRAC6, aucun serveur TFTP n'est requis.

Le protocole simplifié de transfert de fichiers (TFTP) est une forme simplifiée du protocole FTP. Il est utilisé avec les interfaces de ligne de commande SM-CLP et RACADM pour transférer des fichiers à destination et en provenance d'iDRAC6.

Vous devez uniquement copier des fichiers à destination ou en provenance d'iDRAC6 lorsque vous mettez à jour le micrologiciel iDRAC6 ou installez des certificats sur iDRAC6. Si vous choisissez d'utiliser RACADM lorsque vous effectuez ces tâches, un serveur TFTP doit s'exécuter sur un ordinateur auquel iDRAC6 peut avoir accès via l'adresse IP ou le nom DNS.

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

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

Installation de Dell OpenManage IT Assistant

Votre système inclut le kit Dell OpenManage System Management Software. Ce kit inclut, mais sans limitation, les composants suivants :

- 1 DVD *Dell Systems Management Tools and Documentation*

- 1 Site Web du support de Dell et fichiers « Lisez-moi » : consultez les fichiers « Lisez-moi » et le site Web du support de Dell à l'adresse support.dell.com/manuals pour obtenir les dernières informations sur vos produits Dell.

Pour des informations sur l'installation d'IT Assistant, consultez le *Guide d'utilisation de Dell OpenManage IT Assistant* disponible à l'adresse support.dell.com/manuals.

Installation de Dell Management Console

Dell Management Console (DMC) est l'application de gestion de systèmes « un à plusieurs » de nouvelle génération qui intègre des fonctionnalités identiques à celles de Dell OpenManage IT Assistant, en incluant en outre des fonctionnalités de détection, d'inventaire, de surveillance et de génération de rapports améliorées. Il s'agit d'une interface utilisateur graphique (IUG) Web, installée sur une station de gestion dans un environnement mis en réseau.

Vous pouvez installer DMC à partir du DVD *Dell Management Console* ou le télécharger et l'installer à partir du site Web de Dell à l'adresse www.dell.com/openmanage.

Consultez le *Guide d'utilisation de Dell Management Console* disponible à l'adresse support.dell.com/manuals pour obtenir des instructions concernant l'installation de ce logiciel.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration du serveur géré

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Installation du logiciel sur le serveur géré](#)
- [Configuration du serveur géré pour la capture de l'écran de la dernière panne](#)
- [Désactivation de l'option Redémarrage automatique de Windows](#)

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

Installation du logiciel sur le serveur géré

Le logiciel de gestion Dell inclut les fonctionnalités suivantes :

- 1 CLI RACADM : permet de configurer et d'administrer iDRAC6. Il s'agit d'un outil puissant permettant d'écrire des scripts de configuration et de gestion des tâches.
- 1 Server Administrator : permet de tirer parti de la fonctionnalité Écran de la dernière panne iDRAC6.
- 1 Server Administrator Instrumentation Service : permet d'accéder aux informations détaillées sur les anomalies et les performances recueillies par les agents Systems Management standard du secteur et autorise l'administration à distance des systèmes surveillés, y compris l'arrêt, le démarrage et la sécurité.
- 1 Server Administration Storage Management Service : fournit des informations sur Storage Management dans un affichage graphique intégré.
- 1 Journaux Server Administrator : affichent des journaux de commandes émises sur ou par le système, d'événements de matériel surveillés, d'événements POST et d'alertes du système. Vous pouvez afficher les journaux sur la page d'accueil, les imprimer ou les enregistrer comme rapports, puis les envoyer par e-mail à un contact de service désigné.

Utilisez le DVD *Dell Systems Management Tools and Documentation* pour installer Dell OpenManage Server Administrator .Pour des instructions sur l'installation de ce logiciel, consultez le *Guide d'installation de Dell OpenManage Server Administrator* disponible à l'adresse support.dell.com/manuals.

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

iDRAC6 peut capturer l'écran de la dernière panne afin que vous puissiez l'afficher dans l'interface Web et déterminer l'origine du problème du serveur géré et y remédier. Procédez comme suit pour activer la fonctionnalité Écran de la dernière panne.

1. Installez le logiciel Managed Server. Pour de plus amples informations, consultez le *Guide d'installation de Dell OpenManage Server Administrator* et le *Guide d'installation de Dell OpenManage Management Station Software*. Vous pouvez accéder à ces documents sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

2. Si vous travaillez sous Windows, assurez-vous que **Redémarrage automatique** est désélectionné dans les **paramètres de démarrage et de récupération de Windows**. Consultez [Désactivation de l'option Redémarrage automatique de Windows](#).

3. Activez l'**écran de la dernière panne** (désactivé par défaut) dans l'interface Web iDRAC6.

Pour activer l'**écran de la dernière panne** dans l'interface Web iDRAC6, cliquez sur **Système** → **Accès à distance** → iDRAC6 → onglet **Réseau/Sécurité** → **Services**, puis cochez la case **Activé** sous l'en-tête Paramètres de l'**agent de récupération automatique du système**.

Pour activer l'écran de la dernière panne via la RACADM locale, ouvrez une invite de commande sur le serveur géré et entrez la commande suivante :

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

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

Pour des informations sur la configuration de l'horloge de **récupération automatique**, consultez le *Guide d'utilisation de Dell OpenManage Server Administrator*. Pour que l'écran de la dernière panne soit capturé, l'horloge de **récupération automatique** doit être définie sur 60 secondes. Le paramètre par défaut est 480 secondes.

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

Désactivation de l'option Redémarrage automatique de Windows

Pour s'assurer qu'iDRAC6 peut capturer l'écran de la dernière panne, désactivez l'option **Redémarrage automatique** sur les serveurs gérés exécutant Windows Server ou Windows Vista.

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

3. Sous **Démarrage et récupération**, cliquez sur **Paramètres**.
4. Décochez la case **Redémarrage automatique**.
5. Cliquez deux fois sur **OK**.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration d'iDRAC6 Enterprise via l'interface Web

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Accès à l'interface Web](#)
- [Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques](#)
- [Configuration du NIC de l'iDRAC6](#)
- [Configuration et gestion des certificats Microsoft Active Directory](#)
- [Configuration des événements sur plateforme](#)
- [Activation ou désactivation de l'accès à la configuration locale](#)
- [Configuration IPMI sur le LAN](#)
- [Configuration des services iDRAC6](#)
- [Ajout et configuration d'utilisateurs iDRAC6](#)
- [Mise à jour du micrologiciel iDRAC6](#)

iDRAC6 intègre une interface Web qui vous permet de configurer les propriétés et les utilisateurs iDRAC6, d'effectuer les tâches de gestion à distance et de dépanner un système (géré) distant en cas de problème. Vous utiliserez généralement l'interface Web pour exécuter vos tâches quotidiennes de gestion de systèmes. Ce chapitre décrit comment effectuer les tâches de gestion de systèmes courantes en utilisant l'interface Web iDRAC6 et vous procure des liens vers des informations connexes.

La plupart des tâches de configuration que vous exécutez habituellement via l'interface Web peuvent également être effectuées avec des commandes RACADM locale ou distante ou avec des commandes SM-CLP.

Les commandes RACADM locales sont exécutées à partir du serveur géré. La RACADM distante est un utilitaire client qui s'exécute sur une station de gestion et fait appel à l'interface hors bande pour communiquer avec le serveur géré. Cet utilitaire est utilisé avec l'option `-r` pour exécuter des commandes sur un réseau. Pour plus d'informations sur la RACADM, consultez [Utilisation de l'interface de ligne de commande RACADM](#).

Les commandes SM-CLP sont exécutées dans un environnement accessible à distance via une connexion Telnet ou SSH (Secure Shell). Pour plus d'informations sur SM-CLP, consultez [Utilisation d'iDRAC6 Enterprise Interface de ligne de commande SM-CLP](#).

Accès à l'interface Web

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

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Dans le champ **Adresse**, entrez `https://<adresse IP iDRAC6>` et appuyez sur `<Entrée>`.

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

```
https://<adresse IP iDRAC6>:<numéro de port>
```

où *adresse IP iDRAC6* est l'adresse IP pour iDRAC6 et *numéro de port* est le numéro de port HTTPS.

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

Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur iDRAC6, utilisateur Microsoft Active Directory ou utilisateur LDAP. Par défaut, le nom d'utilisateur est **root** et le mot de passe est **calvin**.

Le privilège **Ouverture de session iDRAC** doit vous avoir été octroyé par l'administrateur pour que vous puissiez ouvrir une session iDRAC6.

Pour ouvrir une session, suivez les étapes suivantes :

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

1. Votre nom d'utilisateur iDRAC6.



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

1. Votre nom d'utilisateur Active Directory (AD). Le nom de domaine AD peut également être sélectionné dans le menu déroulant.

Vous pouvez utiliser l'une ou l'autre des formes suivantes en guise de noms Active Directory : `<domaine>\<nom d'utilisateur>`, `<domaine>/<nom d'utilisateur>` ou `<utilisateur>@<domaine>`. Ils ne sont pas sensibles à la casse. Les exemples sont `de11.com\john_doe` ou `JOHN_DOE@DELL.COM`. Vous pouvez également spécifier le domaine dans le champ **Domaine**.

1. Nom d'utilisateur LDAP (sans nom de domaine).

2. Dans le champ **Mot de passe**, saisissez votre mot de passe d'utilisateur iDRAC6, votre mot de passe d'utilisateur Active Directory ou votre mot de passe LDAP. Les mots de passe sont sensibles à la casse.
3. Cliquez sur **OK** ou appuyez sur `<Entrée>`.

Fermeture de session

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

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

 **REMARQUE :** Lorsque le navigateur est fermé sans avoir préalablement fermé la session, la session peut rester ouverte jusqu'à ce qu'elle expire. Il est recommandé de cliquer sur le bouton **Fermer la session** pour mettre fin à une session.

 **REMARQUE :** La fermeture de l'interface Web iDRAC6 dans Internet Explorer à l'aide du bouton Fermer (« x ») en haut à droite de la fenêtre peut générer une erreur d'application. Pour résoudre ce problème, téléchargez la dernière version de Cumulative Security Update for Internet Explorer à partir du site Web du support de Microsoft à l'adresse support.microsoft.com.

 **PRÉCAUTIONS :** 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. Internet Explorer (IE) 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 droits d'utilisateur privilégié sur un onglet, puis qu'il ouvre une session en tant qu'administrateur sur un autre onglet, les deux onglets ouverts possèdent alors des droits d'administrateur.

Le comportement des onglets dans Firefox 2 et Firefox 3 est le même que dans IE 7 et IE 8 ; les nouveaux onglets correspondent à de nouvelles sessions. Le comportement des fenêtres dans Firefox est différent. Les fenêtres de Firefox fonctionnent avec les mêmes privilèges que la dernière fenêtre ouverte. Par exemple, si une seule fenêtre Firefox est ouverte avec un utilisateur privilégié ayant ouvert une session et qu'une autre fenêtre est ouverte avec des droits d'administrateur, les deux utilisateurs auront désormais des droits d'administrateur.

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

Navigateur	Comportement des onglets	Comportement des fenêtres
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 de l'iDRAC6

Cette section suppose qu'iDRAC6 a déjà été configuré et est accessible sur le réseau. Consultez [Configurer la mise en réseau iDRAC6](#) pour obtenir de l'aide sur la configuration réseau d'iDRAC6 initiale.

Configuration des paramètres réseau, IPMI et VLAN

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

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

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6.
2. Cliquez sur l'onglet **Réseau/Sécurité**.
L'écran **Réseau** apparaît.
3. Apportez les modifications nécessaires aux paramètres réseau, IPMI et VLAN. Consultez [Tableau 5-2](#), [Tableau 5-3](#) et [Tableau 5-4](#) pour en savoir plus sur les options **Paramètres réseau**, **IPMI** et **VLAN**.
4. Cliquez sur **Appliquer**.
5. Cliquez sur le bouton approprié pour continuer.

Tableau 5-2. Paramètres réseau

--	--

Paramètre	Description
Paramètres de la carte d'interface réseau	
Adresse Mac	Affiche l'adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nud d'un réseau. L'adresse MAC ne peut pas être modifiée.
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. Par défaut : décoché .
Paramètres communs	
Enregistrer l'iDRAC6 auprès du DNS	Enregistre le nom iDRAC6 sur le serveur DNS. Par défaut : décoché .
DNS iDRAC6 Nom	Affiche le nom iDRAC6. Le nom par défaut est <code>idrac-numéro_de_service</code> , où <code>numéro_de_service</code> est le numéro de service du serveur Dell. Par exemple : <code>iDRAC-HM8912S</code> .
Utiliser DHCP pour le nom de domaine DNS	Coché : acquisition du nom de domaine DNS à partir de DHCP activée. Décoché : acquisition du nom de domaine DNS à partir de DHCP désactivée.
Nom de domaine DNS	Le champ Nom de domaine DNS par défaut est vide. Lorsque la case Utiliser DHCP pour le nom de domaine DNS est cochée, cette option est grisée et le champ ne peut pas être modifié.
Paramètres IPv4	
Activé	Active (coché) ou désactive (décoché) la prise en charge du protocole IPv4. L'option Activer le NIC doit être cochée pour activer ce paramètre.
Activer pour DHCP	Si cette case est cochée , Server Administrator obtient l'adresse IP du NIC iDRAC6 à partir du serveur DHCP. Les champs Adresse IP , Masque de sous-réseau et Passerelle sont également désactivés.
Adresse IP	Vous permet de saisir ou de modifier une adresse IP statique pour le NIC iDRAC6. Pour modifier ce paramètre, désélectionnez l'option Activer pour DHCP .
Masque de sous-réseau	Vous permet de saisir ou de modifier un masque de sous-réseau pour le NIC iDRAC6. Pour modifier ce paramètre, désélectionnez l'option Activer pour DHCP .
Passerelle	Vous permet de saisir ou de modifier une passerelle IPv4 statique pour le NIC iDRAC6. Pour modifier ce paramètre, désélectionnez l'option Activer pour DHCP .
Utiliser DHCP pour obtenir des adresses de serveur DNS	Sélectionnez l'option Activer pour DHCP pour obtenir les adresses de serveur DNS en cochant la case 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 Serveur DNS auxiliaire .
Serveur DNS préféré	Permet de saisir ou de modifier une adresse IP statique pour le serveur DNS préféré. Pour modifier ce paramètre, commencez par désélectionner l'option Utiliser DHCP pour obtenir des adresses de serveur DNS .
Serveur DNS auxiliaire	Utilise l'adresse IP du serveur DNS secondaire si Utiliser DHCP pour obtenir des adresses de serveur DNS n'est pas sélectionné. Entrez l'adresse IP 0.0.0.0 s'il n'y a pas de serveur DNS auxiliaire.
Paramètres IPv6	
Activé	Si la case est cochée , IPv6 est activé. Si la case est décochée , IPv6 est désactivé. Par défaut : décoché .
Activer pour l'autoconfiguration	En sélectionnant cette option, vous permettez à l'iDRAC6 d'obtenir l'adresse IPv6 pour le NIC d'iDRAC6 depuis le serveur de protocole de configuration dynamique d'hôte (DHCPv6). L'activation Activer pour l'autoconfiguration désactive et vide également les valeurs statiques d' adresse IPv6 , de longueur du préfixe et de passerelle .
Adresse IPv6	Configure l'adresse IPv6 du NIC d'iDRAC6. Pour modifier ce paramètre, vous devez d'abord désactiver Activer pour l'autoconfiguration en décochant la case correspondante. REMARQUE : Seules deux adresses IPv6 (adresse locale de lien et adresse globale) sont affichées si DHCP IPv6 est configuré dans votre configuration réseau et les 16 adresses IPv6 sont affichées si vous avez configuré votre routeur réseau pour qu'il envoie des messages d'annonce du routeur. REMARQUE : iDRAC6 ne vous permet pas de sauvegarder les paramètres si vous saisissez une adresse IPv6 comportant plus de huit groupes.
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 d'abord désactiver Activer pour l'autoconfiguration en décochant la case correspondante.
Passerelle	Configure la passerelle IPv6 statique pour le NIC d'iDRAC6. Pour modifier ce paramètre, vous devez d'abord désactiver Activer pour l'autoconfiguration en décochant la case correspondante.
Utiliser DHCPv6 pour obtenir des adresses de serveur DNS	Activez DHCP pour obtenir les adresses IPv6 de serveur DNS en cochant la case Utiliser DHCPv6 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 Serveur DNS auxiliaire . La valeur par défaut est Décochée . REMARQUE : Lorsque la case Utiliser DHCPv6 pour obtenir des adresses de serveur DNS est cochée, les adresses IP ne peuvent pas être saisies dans les champs Serveur DNS préféré et Serveur DNS auxiliaire .
Serveur DNS préféré	Configure l'adresse IPv6 statique du serveur DNS préféré. Pour modifier ce paramètre, désélectionnez Utiliser DHCPv6 pour obtenir des adresses de serveur DNS .
Serveur DNS auxiliaire	Configure l'adresse IPv6 statique du serveur DNS auxiliaire. Pour modifier ce paramètre, désélectionnez Utiliser DHCPv6 pour obtenir des adresses de serveur DNS .

Tableau 5-3. Paramètres IPMI

--	--

Paramètre	Description
Activer IPMI sur le LAN	Lorsqu'elle est cochée, cette case indique que le canal LAN IPMI est activé. Par défaut : décoché .
Limite du niveau de privilège du canal	Configure le niveau de privilège maximum, pour l'utilisateur, qui peut être accepté sur le canal LAN. Sélectionnez l'une des options suivantes : Administrateur , Opérateur ou Utilisateur . L'option par défaut est Administrateur .
Clé de cryptage	Configure la clé de cryptage. La clé de cryptage doit se composer d'un nombre pair de caractères hexadécimaux d'un maximum de 40 caractères sans espace. La clé de cryptage IPMI par défaut ne comprend que des zéros.

Tableau 5-4. Paramètres VLAN

Bouton	Description
Activer le n° VLAN	Oui : activé. Non : désactivé. Si cette option est activée, seul le trafic ID du LAN virtuel (VLAN) sera accepté. REMARQUE : Les paramètres VLAN peuvent uniquement être configurés via l'interface Web CMC. iDRAC6 affiche uniquement la condition d'activation actuelle ; vous ne pouvez pas modifier les paramètres via cet écran.
N° VLAN	Champ N° VLAN des champs 802.1g. Affiche une valeur allant de 1 à 4 094, 4 001 à 4 020 exclus.
Priorité	Champ Priorité des champs 802.1g. Sert à identifier la priorité du N° VLAN et affiche une valeur allant de 0 à 7 pour la priorité du VLAN.

Tableau 5-5. Boutons de l'écran Configuration réseau

Bouton	Description
Paramètres avancés	Affiche l'écran Sécurité réseau , vous permettant d'entrer les attributs de la page IP et les attributs de blocage IP.
Imprimer	Imprime les valeurs de Configuration réseau qui apparaissent à l'écran.
Actualiser	Recharge l'écran Réseau .
Appliquer	Enregistre les nouveaux paramètres définis sur l'écran Configuration réseau. REMARQUE : Les modifications des paramètres de l'adresse IP du NIC ferment toutes les sessions utilisateur et forcent les utilisateurs à se reconnecter à l'interface Web iDRAC6 avec les paramètres d'adresse IP mis à jour. Toutes les autres modifications nécessitent la réinitialisation du NIC, qui peut provoquer une perte brève de connectivité.

Configuration du filtrage IP et du blocage IP

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

1. Cliquez sur **Système** → **Accès à distance** → **iDRAC6**.
2. Cliquez sur l'onglet **Réseau/Sécurité**.
L'écran **Réseau** apparaît.
3. Cliquez sur **Paramètres avancés**.
L'écran **Sécurité réseau** apparaît.
4. Définissez les paramètres de filtrage IP et de blocage IP. Consultez la section [Tableau 5-6](#) pour en savoir plus sur les paramètres de **filtrage IP et de blocage IP**.
5. Cliquez sur **Appliquer**.
6. Cliquez sur le bouton approprié pour continuer. Consultez [Tableau 5-7](#).

Tableau 5-6. Paramètres de filtrage IP et de blocage IP

Paramètres	Description
Plage IP activée	Active la fonctionnalité de vérification de la plage IP, qui définit une plage d'adresses IP pouvant accéder à iDRAC6. La valeur par défaut est Désactivé .
Adresse de la plage IP	Détermine l'adresse de sous-réseau IP acceptée. L'adresse par défaut est 192.168.1.0 .
Masque de sous-réseau de la plage IP	Définit les positions binaires significatives 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 des échecs du nombre d'échecs avant blocage d'IP doivent se produire pour déclencher la période de pénalité avant blocage d'IP. La période par défaut est 3 600 .
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. La période par défaut est 3 600 .

Tableau 5-7. Boutons de l'écran Sécurité réseau

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

Configuration des événements sur plateforme

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

Les événements sur plateforme filtrables sont répertoriés dans [Tableau 5-8](#).

Tableau 5-8. Événements sur plateforme filtrables

Index	Événement sur plateforme
1	Avertissement de capteur de batterie
2	Panne de capteur de batterie
3	Échec discret signalé par le capteur de tension
4	Avertissement de capteur de température
5	Panne de capteur de température
6	Panne de processeur
7	Processeur absent
8	Erreur dans le journal du matériel
9	Récupération automatique du système
10	Défaillance de la carte SD
11	Perte de la redondance

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

Si le même filtre d'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.

- Ouvrez une session sur l'interface Web iDRAC6.
- Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.
L'écran **Événements sur plateforme** apparaît.
- Cochez la case **Activer les alertes de filtre d'événements sur plateforme**. Vous devez sélectionner cette option pour toute alerte de plateforme à envoyer à une destination valide.
- Sélectionnez l'une des actions suivantes que vous voulez activer pour chaque événement :
 - Redémarrer le système : lorsqu'un événement se produit, le système redémarre (démarrage à chaud).

- 1 Exécuter un cycle d'alimentation sur le système : lorsqu'un événement se produit, le système s'arrête, se met hors tension, puis redémarre (démarrage à froid).
 - 1 Mettre le système hors tension : lorsqu'un événement se produit, le système s'arrête et se met hors tension.
 - 1 Pas d'action : lorsqu'un événement se produit, aucune action n'est effectuée. Il s'agit du paramètre par défaut pour un événement.
5. Sélectionnez l'option **Générer une alerte** en regard de chacun des événements pour lesquels vous souhaitez déclencher une alerte.

 **REMARQUE :** Vous pouvez activer ou désactiver la génération d'une alerte pour tous les événements en cochant ou décochant la case située en regard de l'en-tête de colonne **Générer une alerte**.

6. Cliquez sur **Appliquer**.

Configuration des interruptions d'événement sur plateforme (PET)

 **REMARQUE :** Vous devez disposer de l'autorisation **Configurer iDRAC** pour ajouter ou activer/désactiver une alerte SNMP. Les options suivantes ne sont pas disponibles si vous ne disposez pas de l'autorisation **Configurer iDRAC**.

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Assurez-vous d'avoir bien suivi les procédures dans [Configuration des filtres d'événements sur plateforme \(PEF\)](#).
3. Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.

L'écran **Événements sur plateforme** apparaît.

4. Cliquez sur **Paramètres des interruptions**.

L'écran **Paramètres des interruptions** apparaît.

5. Configurez votre adresse IP de destination PET :
 - a. Cochez la case **Activé** en regard du **Numéro de destination** que vous voulez activer.
 - b. Saisissez une adresse IP dans la zone **Adresse IP de destination IPv4 ou IPv6** appropriée.
 - c. Cliquez sur **Appliquer**.

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

- d. Pour tester l'alerte configurée, cliquez sur **Envoyer**.
- e. Pour ajouter une adresse IP de destination supplémentaire, recommencez les étapes [étape a](#) à [étape d](#). Vous pouvez spécifier jusqu'à quatre adresses IPv4 de destination et quatre adresses IPv6 de destination.

Configuration des alertes par e-mail

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Assurez-vous d'avoir bien suivi les procédures dans [Configuration des filtres d'événements sur plateforme \(PEF\)](#).
3. Cliquez sur **Système**, puis sur l'onglet **Gestion des alertes**.

L'écran **Événements sur plateforme** apparaît.

4. Cliquez sur **Paramètres d'alertes par e-mail**.

L'écran **Paramètres d'alertes par e-mail** apparaît.

5. Configurez votre destination des alertes par e-mail.
 - a. Cochez la case **Activé** correspondant à la première alerte par e-mail non définie.
 - b. Saisissez une adresse e-mail valide dans le champ **Adresse e-mail de destination**.
 - c. Cliquez sur **Appliquer**.

 **REMARQUE :** Pour réussir à envoyer un e-mail test, le serveur SMTP (e-mail) doit être configuré dans la section **Paramètres d'adresses du serveur SMTP (e-mail)** de l'écran **Paramètres d'alertes par e-mail**. Spécifiez un serveur SMTP dans le champ fourni en utilisant le format séparé

par un point (par exemple, 192.168.1.1) ou le nom DNS. L'adresse IP du serveur SMTP communique avec iDRAC6 pour envoyer des alertes par e-mail lorsqu'un événement sur plateforme se produit.

- d. Dans le champ **Modifier le nom de l'e-mail source**, saisissez l'e-mail de l'expéditeur pour l'alerte ou laissez le champ vide pour utiliser l'expéditeur de l'e-mail par défaut. La valeur par défaut est `logement_lame@Adresse IP iDRAC6`.
 - o Si le champ **Modifier le nom de l'e-mail source** est vide, le nom d'hôte iDRAC6 est configuré et le nom de domaine DNS est actif, puis l'adresse e-mail source est : `<Nom d'hôte iDRAC6>@<Nom de domaine DNS>`.
 - o Si le champ est vide, que le nom d'hôte d'iDRAC6 est vierge et que le nom de domaine DNS est actif, l'adresse e-mail source est alors : `<Logementx d'iDRAC6>@<Nom de domaine DNS>`.
 - o Si le champ est vide, que le nom d'hôte iDRAC6 est vierge et que le nom de domaine DNS est vierge, l'adresse e-mail source est alors : `<Logementx iDRAC6>@<Adresse IP iDRAC6>`.
 - o Si le champ est « **une chaîne sans @** » et que le nom de domaine DNS est actif, l'adresse e-mail source est alors : `<une chaîne sans @>@<Nom de domaine DNS>`.
 - o Si le champ est « **une chaîne sans @** » et que le nom de domaine DNS est vierge, l'adresse e-mail source est alors : `<une chaîne sans @>@<Adresse IP iDRAC6>`.
 - o Si le champ est « **une chaîne avec @** » et que le nom de domaine DNS est actif, l'adresse e-mail source est alors : `<une chaîne avec @>@<Nom de domaine DNS>`.
 - o Si le champ est « **une chaîne avec @** » et que le nom de domaine DNS est vierge, l'adresse e-mail source est alors : `<une chaîne avec @>@<Adresse IP iDRAC6>`.
- e. Cliquez sur **Envoyer** pour tester l'alerte par e-mail configurée (si nécessaire).
- f. Pour ajouter une destination d'alerte par e-mail supplémentaire, répétez [étape a](#) à [étape e](#). Vous pouvez spécifier jusqu'à quatre destinations d'alerte par e-mail.

Configuration IPMI sur le LAN

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Configurez IPMI sur le LAN :
 - a. Cliquez sur **Système** → **Accès à distance** → iDRAC6, puis cliquez sur l'onglet **Réseau/Sécurité**.

L'écran **Réseau** apparaît.

- b. Cliquez sur **Paramètres IPMI**.
- c. Cochez la case **Activer IPMI sur le LAN**.
- d. Mettez à jour la **Limite du niveau de privilège du canal**, si nécessaire :

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

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

- f. Cliquez sur **Appliquer**.

3. Configurez Communications série IPMI sur le LAN (SOL) :
 - a. Cliquez sur **Système** → **Accès à distance** → iDRAC6, puis cliquez sur l'onglet **Réseau/Sécurité**.

L'écran **Réseau** apparaît.

- b. Cliquez sur l'onglet **Communications série sur le LAN**.
- c. Sélectionnez **Activer les communications série sur le LAN**.
- d. Mettez à jour le **débit en bauds** SOL IPMI, si nécessaire, en sélectionnant une vitesse de données dans le menu déroulant **Débit en bauds**.

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

- e. Cliquez sur **Appliquer**.
 - f. Configurez les paramètres de filtrage IP et de blocage IP selon les besoins dans la page **Paramètres avancés**.
-

Ajout et configuration d'utilisateurs iDRAC6

Pour gérer votre système avec iDRAC6 et maintenir la sécurité du système, créez des utilisateurs uniques et octroyez-leur des droits d'administration spécifiques (ou *autorité basée sur les rôles*).

Pour ajouter et configurer des utilisateurs iDRAC6, suivez les étapes suivantes :

 **REMARQUE :** Vous devez disposer du droit **Configurer iDRAC** pour effectuer les étapes suivantes.

1. Cliquez sur **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Utilisateurs**.

L'écran **Utilisateurs** affiche la **Réf. utilisateur, l'état, le nom d'utilisateur, les privilèges LAN IPMI** de chaque utilisateur, les privilèges iDRAC6 et les **communications série sur le LAN**.

 **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.
3. Sur la page **Menu principal utilisateur** (consultez [Tableau 5-9](#), [Tableau 5-10](#) et [Tableau 5-11](#)), vous pouvez configurer un utilisateur, téléverser un fichier de clé publique SSH ou bien afficher ou supprimer une clé SSH spécifiée ou toutes les clés SSH.

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 la PKA sur SSH est configurée et utilisée correctement, vous n'avez pas à saisir le mot de passe lors de l'ouverture de 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 :

1. Vous pouvez gérer cette fonctionnalité à l'aide de la RACADM et également depuis l'IUG.
1. 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 fournit 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. Saisissez le nombre de bits de la clé. RSA et DSA sont les seuls algorithmes de génération de clé pris en charge. Le 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 en utilisant l'option **Enregistrer la clé publique** pour la téléverser ultérieurement. Toutes les clés téléversées doivent être au format RFC 4716 ou openSSH. Dans le cas contraire, vous devez convertir ces clés dans ces formats.

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

-t peut être *dsa* ou *rsa*.

-b spécifie la taille du cryptage binaire entre 768 et 4 096.

-C permet de modifier le commentaire de la clé publique et est facultative.

Une fois la commande exécutée, téléversez le fichier public.

 **REMARQUE :** Les clés générées depuis la station de gestion Linux à l'aide de `ssh-keygen` ne sont pas au format RFC4716, mais au format openSSH. Les clés publiques openSSH peuvent être téléversées sur iDRAC6. L'algorithme de clé publique iDRAC6 valide les clés openSSH et RFC4716, convertit en interne les clés RFC4716 au format openSSH, puis stocke les clés en interne.

 **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 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
```

Consultez [Téléversement, affichage et suppression de clés SSH avec la RACADM](#) pour des informations sur le téléversement, l'affichage et la suppression des clés SSH à l'aide de la RACADM.

Tableau 5-9. 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. Si une clé est téléversée, le contenu du fichier de clé s'affiche dans une zone de texte non modifiable de la page Configuration utilisateur .
Afficher/Supprimer les clés SSH	Permet à l'utilisateur local d'afficher ou de supprimer une clé SSH spécifiée ou toutes les clés SSH.

La page **Téléverser des clés SSH** vous permet de téléverser un fichier de clé publique SSH. Si une clé est téléversée, le contenu du fichier de clé est affiché dans une zone de texte non modifiable sur la page **Afficher/Supprimer les clés SSH**.

 **PRÉCAUTIONS :** La capacité à téléverser, à afficher et/ou à supprimer les clés SSH est basée sur le privilège utilisateur « Configurer les utilisateurs ». Ce privilège permet aux utilisateurs de configurer la clé SSH d'un autre utilisateur. Vous devez accorder ce privilège avec prudence. Pour plus d'informations, consultez [Tableau 5-14](#).

Tableau 5-10. 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 . REMARQUE : L'option de collage du texte de la clé est prise en charge pour les clés publiques au format openSSH. L'option de collage du texte pour la clé au format RFC4716 n'est pas prise en charge.
Parcourir	Cliquez sur ce bouton pour identifier le chemin complet et le nom de fichier de la clé.

La page **Afficher/Supprimer les clés SSH** vous permet d'afficher ou de supprimer les clés publiques SSH de l'utilisateur.

Tableau 5-11. Afficher/Supprimer les 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.

1. Si vous sélectionnez **Configurer l'utilisateur** et cliquez sur **Suivant**, la page Configuration utilisateur apparaît.
2. Sur l'écran **Configuration utilisateur**, définissez les propriétés et les privilèges de l'utilisateur.
 - [Tableau 5-12](#) décrit les paramètres **généraux** pour configurer un nom d'utilisateur et un mot de passe iDRAC6.
 - [Tableau 5-13](#) décrit les **Privilèges LAN IPMI** pour la configuration des privilèges LAN de l'utilisateur.
 - [Tableau 5-14](#) décrit les droits du groupe Utilisateurs pour les paramètres **Privilèges LAN IPMI** et **Privilèges utilisateur** iDRAC6.
 - [Tableau 5-15](#) décrit les droits du groupe iDRAC6. Si vous ajoutez un **privilège utilisateur iDRAC6** à **Administrateur**, **Utilisateur privilégié** ou **Utilisateur invité**, le groupe iDRAC6 bascule sur le groupe **Personnalisé**.
3. Lorsque vous avez terminé, cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Consultez [Tableau 5-16](#).

Tableau 5-12. Propriétés générales

Propriété	Description																								
Réf. utilisateur	Contient l'un des 16 numéros d'identification prédéfinis. Ce champ ne peut pas être modifié.																								
Activer l'utilisateur	Lorsqu'elle est cochée , cette propriété indique que l'accès de l'utilisateur à iDRAC6 est activé. Lorsqu'elle est décochée , l'accès utilisateur est désactivé.																								
Nom d'utilisateur	Spécifie un nom d'utilisateur iDRAC6 contenant jusqu'à 16 caractères. Chaque utilisateur doit avoir un nom d'utilisateur unique. <ul style="list-style-type: none"> 1 0-9 1 A-Z 1 a-z 1 Caractères spéciaux : <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">+</td><td style="width: 12.5%;">%</td><td style="width: 12.5%;">=</td><td style="width: 12.5%;">,</td><td style="width: 12.5%;">-</td><td style="width: 12.5%;">{</td><td style="width: 12.5%;">}</td><td style="width: 12.5%;">\$</td></tr> <tr> <td>!</td><td>(</td><td>?</td><td>;</td><td>_</td><td>}</td><td> </td><td></td></tr> <tr> <td>#</td><td>)</td><td>*</td><td>:</td><td>\$</td><td>[</td><td> </td><td></td></tr> </table> <p>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.</p>	+	%	=	,	-	{	}	\$!	(?	;	_	}			#)	*	:	\$	[
+	%	=	,	-	{	}	\$																		
!	(?	;	_	}																				
#)	*	:	\$	[
Modifier le mot de passe	Active les champs Nouveau mot de passe et Confirmer le nouveau mot de passe . Lorsque cette option n'est pas sélectionnée, le mot de passe de l'utilisateur ne peut pas être modifié.																								
Nouveau mot de passe	Active la modification du mot de passe de l'utilisateur iDRAC6. Saisissez un mot de passe de 20 caractères maximum. Les caractères ne seront pas affichés. <ul style="list-style-type: none"> 1 0-9 1 A-Z 1 a-z 1 Caractères spéciaux : <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">+</td><td style="width: 12.5%;">%</td><td style="width: 12.5%;">=</td><td style="width: 12.5%;">,</td><td style="width: 12.5%;">-</td><td style="width: 12.5%;">{</td><td style="width: 12.5%;">}</td><td style="width: 12.5%;">.</td></tr> <tr> <td>!</td><td>(</td><td>?</td><td>;</td><td>_</td><td>}</td><td> </td><td> </td></tr> <tr> <td>#</td><td>)</td><td>*</td><td>:</td><td>\$</td><td>[</td><td>/</td><td>@</td></tr> </table>	+	%	=	,	-	{	}	.	!	(?	;	_	}			#)	*	:	\$	[/	@
+	%	=	,	-	{	}	.																		
!	(?	;	_	}																				
#)	*	:	\$	[/	@																		
Confirmer le nouveau mot de passe	Saisissez à nouveau le mot de passe de l'utilisateur iDRAC6 pour confirmer.																								

Tableau 5-13. Privilège LAN 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 : Aucun , Administrateur , Opérateur ou Utilisateur .
Activation des communications série sur le LAN	Permet à l'utilisateur d'utiliser les communications série sur le LAN IPMI. Lorsque cette option est sélectionnée , ce privilège est activé.

Tableau 5-14. Autre privilège

Propriété	Description

Propriété	Description
Groupe iDRAC6	Définit le privilège utilisateur iDRAC6 maximal comme l'une des options suivantes : Administrateur , Utilisateur privilégié , Utilisateur invité , Personnalisé ou Aucun . Consultez la section Tableau 5-15 pour connaître les droits Groupe iDRAC6.
Ouvrir une session iDRAC6	Permet à l'utilisateur d'ouvrir une session iDRAC6.
Configurer iDRAC6	Permet à l'utilisateur de configurer iDRAC6.
Configurer les utilisateurs	Permet à l'utilisateur de permettre à des utilisateurs spécifiques d'accéder au système. PRÉCAUTIONS : Ce privilège est généralement réservé aux utilisateurs qui sont membres du groupe d'utilisateurs Administrateur sur iDRAC. Les utilisateurs du groupe d'utilisateurs « Personnalisé » peuvent toutefois bénéficier de ce privilège. Un utilisateur possédant ce privilège peut modifier la configuration de n'importe quel utilisateur. Ceci inclut la création ou la suppression de n'importe quel utilisateur, la gestion des clés SSH des utilisateurs, etc. Pour ces raisons, vous devez attribuer ce privilège avec prudence.
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 console virtuelle	Permet à l'utilisateur d'exécuter la console virtuelle. PRÉCAUTIONS : Ce privilège est généralement réservé aux utilisateurs qui sont membres du groupe Administrateur ou Utilisateur privilégié sur iDRAC. En plus de pouvoir utiliser la console virtuelle, les utilisateurs disposant du privilège Accéder à la console virtuelle sont autorisés à afficher dans l'interface Web iDRAC6 les activités de tout utilisateur utilisant la console virtuelle. Pour ces raisons, vous devez attribuer ce privilège avec prudence.
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 de test (e-mail et PET) à tous les destinataires d'alerte actuellement configurés.
Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Tableau 5-15. Droits du groupe iDRAC6

Groupe d'utilisateurs	Droits accordés
Administrateur	Ouvrir une session iDRAC6, Configurer iDRAC6, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du serveur , Accès à la console virtuelle , Accès au média virtuel , Tester les alertes, Exécution des commandes de diagnostic
Utilisateur privilégié	Ouvrir une session iDRAC6, Effacer les journaux, Exécuter des commandes de contrôle du serveur , Accès à la console virtuelle , Accès au média virtuel , Tester les alertes
Utilisateur invité	Ouvrir une session iDRAC6
Personnalisé	Sélectionne toute combinaison des autorisations suivantes : Ouvrir une session iDRAC6, Configurer iDRAC6, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du serveur , Accès à la console virtuelle , Accès au média virtuel , Tester les alertes, Exécution des commandes de diagnostic
Aucune	Aucun droit attribué

Tableau 5-16. Boutons de l'écran Configuration utilisateur

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

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 iDRAC6 :

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

- 1 Affichage d'un certificat de serveur

Secure Sockets Layer (SSL)

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

Un système activé SSL peut effectuer les tâches suivantes :

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

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

Le serveur Web iDRAC6 dispose d'un certificat numérique SSL autosigné Dell (référence serveur) par défaut. Pour garantir un niveau de sécurité élevé sur Internet, remplacez le certificat SSL Web Server par un certificat signé par une autorité de certification connue. Une autorité de certification est une entité commerciale reconnue dans l'industrie de l'informatique pour ses critères élevés en matière d'analyse fiable et d'identification, et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'AC. Pour lancer le processus d'obtention d'un certificat signé, vous pouvez utiliser l'interface Web iDRAC6 pour générer une requête de signature de certificat (RSC) avec les informations de votre société. Vous pouvez ensuite envoyer la RSC générée à une autorité de certification telle que VeriSign ou Thawte.

Requête de signature de certificat (RSC)

Une RSC est une requête numérique adressée à une autorité de certification (AC) pour un certificat de serveur sécurisé. Les certificats de serveur sécurisés permettent aux clients du serveur de faire confiance à l'identité du serveur et de négocier une session cryptée avec le serveur.

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'autorité de certification, cette dernière lui envoie un certificat signé numériquement qui identifie de manière exclusive le postulant pour les transactions effectuées sur des réseaux et sur Internet.

Une fois que l'autorité de certification approuve la RSC et qu'elle envoie le certificat, téléversez ce dernier sur le micrologiciel iDRAC6. Les informations de la RSC enregistrées sur le micrologiciel iDRAC6 doivent correspondre aux informations du certificat. En d'autres termes, le certificat doit avoir été généré en réponse à la RSC créée par l'iDRAC6.

Accès au menu principal SSL

1. Cliquez sur **Système** → **Accès à distance** → **iDRAC6** → onglet **Réseau/Sécurité**.
2. Cliquez sur **SSL** pour accéder à l'écran **SSL**.

[Tableau 5-17](#) décrit les options disponibles lors de la génération d'une RSC.

[Tableau 5-18](#) décrit les boutons disponibles dans l'écran Menu principal SSL.

Tableau 5-17. Options du menu principal SSL

Champ	Description
Générer une nouvelle requête de signature de certificat (RSC)	Sélectionnez l'option et cliquez sur Suivant pour accéder à l'écran Générer une requête de signature de certificat (RSC) . REMARQUE : Chaque nouvelle RSC supprime la RSC 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 un certificat de serveur	Sélectionnez l'option et cliquez sur Suivant pour accéder à l'écran Téléversement d'un certificat et téléverser le certificat que vous a envoyé l'autorité de certification. REMARQUE : iDRAC6 accepte uniquement les certificats X509, encodés en base 64. Les certificats encodés DER ne sont pas acceptés.
Afficher le certificat de serveur	Sélectionnez l'option et cliquez sur Suivant pour accéder à l'écran Afficher le certificat de serveur et afficher le certificat de serveur existant.

Tableau 5-18. Boutons du menu principal SSL

Bouton	Description

Imprimer	Imprime les valeurs SSL qui apparaissent à l'écran.
Actualiser	Recharge l'écran SSL.
Suivant	Traite les informations sur l'écran SSL et passe à l'étape suivante.

Génération d'une nouvelle requête de signature de certificat

REMARQUE : La nouvelle RSC remplace toujours les données de RSC stockées sur le micrologiciel. La RSC présente dans le micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification. Sinon, iDRAC6 n'acceptera pas le certificat.

1. Dans l'écran SSL, sélectionnez **Générer une nouvelle requête de signature de certificat (RSC)** et cliquez sur **Suivant**.

2. Dans l'écran **Générer une requête de signature de certificat (RSC)**, entrez une valeur pour chaque attribut RSC.

[Tableau 5-19](#) décrit les options de l'écran **Générer une requête de signature de certificat (RSC)**.

3. Cliquez sur **Générer** pour créer la requête de signature de certificat.

4. Cliquez sur **Télécharger** pour enregistrer le fichier RSC sur votre station de gestion distante.

5. Cliquez sur le bouton approprié pour continuer. Consultez [Tableau 5-20](#).

Tableau 5-19. Options de l'écran **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.sociétéxyz.com). Seuls les caractères alphanumériques, les espaces, les tirets, les traits de soulignement 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.
Service de l'organisation	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. Entrez l'adresse e-mail de l'entreprise ou toute autre adresse e-mail associée à la RSC. Ce champ est optionnel.
Taille de la clé	La taille de la clé de requête de signature de certificat (RSC) à générer. La taille est 1 024 Ko ou 2 048 Ko.

Tableau 5-20. Boutons de l'écran **Générer une requête de signature de certificat (RSC)**

Bouton	Description
Imprimer	Imprime les valeurs de Générer une requête de signature de certificat (RSC) qui apparaissent à l'écran.
Actualiser	Recharge la page Générer une requête de signature de certificat (RSC) .
Générer	Génère une RSC puis invite l'utilisateur à l'enregistrer dans un répertoire spécifié.
Télécharger	Télécharge le certificat sur l'ordinateur local.
Retour au menu principal SSL	Renvoie l'utilisateur à l'écran SSL.

Téléversement d'un certificat de serveur

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

L'écran **Téléversement d'un certificat** apparaît.

2. Dans le champ **Chemin de fichier**, entrez le chemin d'accès au certificat ou cliquez sur **Parcourir** pour accéder au fichier de certificat sur la station de gestion.

REMARQUE : La valeur **Chemin de fichier** affiche le chemin de fichier du certificat que vous téléversez. Vous devez entrer le chemin de fichier, c'est-à-dire le chemin d'accès et le nom de fichier complets ainsi que l'extension du fichier.

3. Cliquez sur **Appliquer**.

4. Cliquez sur le bouton approprié pour continuer. Consultez [Tableau 5-21](#).

Tableau 5-21. Boutons de l'écran Téléversement d'un certificat

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

Affichage d'un certificat de serveur

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

[Tableau 5-22](#) décrit les champs et les descriptions associées énumérés dans la fenêtre **Afficher le certificat de serveur**.

2. Cliquez sur le bouton approprié pour continuer. Consultez [Tableau 5-23](#).

Tableau 5-22. Afficher les informations sur le certificat de serveur

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

Tableau 5-23. Boutons de l'écran Afficher le certificat de serveur

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

Configuration et gestion des certificats Microsoft Active Directory

 **REMARQUE :** Vous devez disposer de l'autorisation **Configurer iDRAC** pour configurer Active Directory, et téléverser, télécharger et afficher un certificat Active Directory.

 **REMARQUE :** Pour plus d'informations sur la configuration d'Active Directory et sur la manière de configurer Active Directory avec le schéma standard ou un schéma étendu, consultez [« Utilisation du service d'annuaire iDRAC6 », page 141](#).

Pour accéder à l'écran de résumé Microsoft Active Directory, cliquez sur **Système** → **Accès à distance** → **iDRAC6** → onglet **Réseau/Sécurité** → **Service d'annuaire** → **Microsoft Active Directory**.

[Tableau 5-24](#) répertorie les options du résumé Active Directory. Cliquez sur le bouton approprié pour continuer.

Tableau 5-24. Options d'Active Directory

Champ	Description
Paramètres communs	Affiche les paramètres Active Directory couramment configurés.
Certificat d'AC Active Directory	Affiche le certificat de l'autorité de certification qui signe l'ensemble des certificats de serveur SSL des contrôleurs de domaine.
Paramètres du schéma standard/Paramètres du schéma étendu	En fonction de la configuration actuelle d'Active Directory, les paramètres du schéma étendu ou les paramètres du schéma standard sont affichés.
Configurer Active Directory	Cliquez sur cette option pour configurer l'Étape 1 sur 4 dans Paramètres Active Directory. La page Étape 1 sur 4 Active Directory vous permet de téléverser un certificat d'autorité de certification d'Active Directory dans l'iDRAC6, d'afficher le certificat d'autorité de certification d'Active Directory actuel qui a été téléversé dans l'iDRAC6, ou d'activer la validation des certificats.

Paramètres du test	Cliquez sur cette option pour tester la configuration d'Active Directory à l'aide des paramètres spécifiés.
Téléversement du fichier keytab Kerberos	Cliquez sur cette option pour téléverser le fichier keytab Kerberos sur iDRAC6. Pour des informations sur la création d'un fichier keytab, consultez Configuration d'iDRAC6 pour la connexion directe et l'ouverture de session par carte à puce .

Tableau 5-25. Boutons d'Active Directory

Bouton	Définition
Imprimer	Imprime les valeurs d'Active Directory qui apparaissent à l'écran.
Actualiser	Recharge l'écran Active Directory.

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

1. Sur l'écran de résumé **Active Directory**, cliquez sur **Configurer Active Directory**.
2. Sur l'écran **Étape 1 sur 4 Active Directory**, vous avez la possibilité d'activer la validation de certificats, de téléverser le certificat d'autorité de certification d'Active Directory dans l'iDRAC6 ou d'afficher le certificat d'autorité de certification d'Active Directory actuel.

[Tableau 5-26](#) décrit les paramètres et les sélections pour chaque étape du processus de configuration et de gestion d'Active Directory. Cliquez sur le bouton approprié pour continuer.

Tableau 5-26. Paramètres de l'écran Configuration d'Active Directory

Paramètre	Description
Étape 1 sur 4 Configuration et gestion d'Active Directory	
Validation de certificat activée	Indique si la validation des certificats est activée ou désactivée. Si cette case est cochée , la validation des certificats est activée. iDRAC6 utilise le protocole LDAP sur un protocole de sécurité de cryptage (SSL) lors de la connexion d'Active Directory. Par défaut, iDRAC6 fournit une sécurité accrue au moyen du certificat de l'autorité de certification chargé dans iDRAC6 pour valider le certificat de serveur SSL des contrôleurs de domaine durant l'établissement de liaisons SSL. La validation des certificats peut être désactivée aux fins de test.
Téléverser le certificat d'autorité de certification d'Active Directory	Pour téléverser un certificat d'autorité de certification d'Active Directory, cliquez sur Parcourir , sélectionnez le fichier, puis cliquez sur Téléverser . Assurez-vous que les certificats SSL du contrôleur de domaine sont signés par la même autorité de certification et que ce certificat est disponible sur la station de gestion accédant à iDRAC6. La valeur Chemin de fichier affiche le chemin de fichier du certificat que vous téléversez. Si vous choisissez de ne pas naviguer jusqu'au certificat, entrez le chemin de fichier, c'est-à-dire le chemin d'accès et le nom de fichier complets ainsi que l'extension du fichier.
Certificat d'autorité de certification d'Active Directory actuel	Affiche le certificat d'autorité de certification d'Active Directory qui a été téléversé dans l'iDRAC6.
Étape 2 sur 4 Configuration et gestion d'Active Directory	
Active Directory activé	Sélectionnez cette option si vous souhaitez activer Active Directory.
Activer la connexion par carte à puce	Sélectionnez cette option pour activer la connexion par carte à puce. Vous serez invité à ouvrir une session par carte à puce lors de chaque tentative ultérieure d'ouverture de session via l'interface utilisateur graphique. REMARQUE : Les fonctionnalités TFA basée sur la carte à puce et de connexion directe sont uniquement prises en charge par les systèmes d'exploitation Microsoft Windows avec Internet Explorer. En outre, les services Terminal Server (Bureau à distance) sous Windows XP ne prennent pas en charge les opérations par carte à puce. Toutefois, Windows Vista prend en charge ces opérations.
Activer la connexion directe	Sélectionnez cette option si vous souhaitez ouvrir une session iDRAC6 sans entrer vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Si vous activez la connexion directe (SSO) puis fermez la session, vous pouvez rouvrir la session à l'aide de SSO. Si vous avez déjà ouvert une session à l'aide de la connexion directe puis fermé votre session ou que la connexion directe échoue, la page de connexion Web normale s'affiche. REMARQUE : L'activation de l'ouverture de session par carte à puce ou de la connexion directe ne désactive pas les interfaces hors bande de ligne de commande, y compris Telnet, SSH, RACADM distante et IPMI sur le LAN. REMARQUE : Dans cette version, la fonctionnalité Authentification bifactorielle (TFA) par carte à puce n'est pas prise en charge si Active Directory est configuré pour le schéma étendu. La fonctionnalité Connexion directe (SSO) est prise en charge à la fois pour le schéma standard et pour le schéma étendu.
Nom de domaine de l'utilisateur	Saisissez les entrées de nom de domaine de l'utilisateur. Si elle est configurée, une liste des noms de domaine d'utilisateur apparaît sur la page d'ouverture de session sous la forme d'un menu déroulant. Si elle n'est pas configurée, les utilisateurs d'Active Directory sont toujours en mesure d'ouvrir une session en entrant le nom d'utilisateur au format nom_d'utilisateur@nom_domaine ou nom_domaine/nom_d'utilisateur. Ajouter : ajoute une nouvelle entrée de nom de domaine utilisateur à la liste. Modifier : modifie une entrée existante de nom de domaine utilisateur. Supprimer : supprime de la liste une entrée de nom de domaine utilisateur.
Délai d'expiration	Entrez la durée maximale, en secondes, accordée aux requêtes Active Directory pour qu'elles se terminent.
Rechercher les contrôleurs de domaine avec DNS	Sélectionnez l'option Rechercher les contrôleurs de domaine avec DNS pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Lorsque cette option est sélectionnée, les adresses des serveurs des contrôleurs de domaine 1 à 3 sont ignorées. Sélectionnez Domaine utilisateur de connexion pour effectuer la recherche DNS avec le nom de domaine de

	<p>L'utilisateur d'ouverture de session. Sinon, sélectionnez Définir un domaine et saisissez le nom de domaine à utiliser pour 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.</p> <p>Si Schéma étendu est sélectionné, ces adresses sont celles des contrôleurs de domaine dans lesquels l'objet Périphérique iDRAC6 et les objets Association sont situés. Si Schéma standard est sélectionné, les contrôleurs de domaine sont ceux où se trouvent les comptes d'utilisateur et les groupes de rôles.</p>
Spécifier les adresses des contrôleurs de domaine	<p>Sélectionnez l'option Définir des adresses de contrôleur de domaine pour autoriser iDRAC6 à utiliser les adresses des serveurs des contrôleurs de domaine Active Directory qui sont spécifiées. Lorsque cette option est sélectionnée, la recherche DNS n'a pas lieu. Spécifiez l'adresse IP ou le nom de domaine pleinement qualifié (FQDN) des contrôleurs de domaine. Lorsque l'option Définir des adresses de contrôleur de domaine est sélectionnée, au moins 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.</p> <p>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. Si Schéma étendu est sélectionné, ces adresses sont celles des contrôleurs de domaine dans lesquelles l'objet Périphérique iDRAC6 et les objets Association sont situés.</p>
Étape 3 sur 4 Configuration et gestion d'Active Directory	
Sélection du schéma étendu	<p>Sélectionnez cette option si vous souhaitez utiliser le schéma étendu avec Active Directory.</p> <p>Cliquez sur Suivant pour afficher la page Étape 4 sur 4 Configuration et gestion d'Active Directory.</p> <p>Nom d'iDRAC6 : spécifie le nom qui identifie de manière unique iDRAC6 dans Active Directory. Cette valeur est NULL par défaut.</p> <p>Nom de domaine iDRAC6 : le nom DNS (chaîne) du domaine où réside l'objet iDRAC d'Active Directory. Cette valeur est NULL par défaut.</p> <p>Ces paramètres s'affichent uniquement si iDRAC6 a été configuré en vue d'une utilisation avec un schéma Active Directory étendu.</p>
Sélection du schéma standard	<p>Sélectionnez cette option si vous souhaitez utiliser le schéma standard avec Active Directory.</p> <p>Cliquez sur Suivant pour afficher la page Étape 4a sur 4 Active Directory.</p> <p>Sélectionnez l'option Rechercher des 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. Lorsque cette option est sélectionnée, les adresses des serveurs de catalogue global 1 à 3 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 requis pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.</p> <p>Sélectionnez l'option Définir des adresses de serveur de catalogue global et saisissez l'adresse IP ou le nom de domaine pleinement qualifié du (des) serveur(s) de catalogue global. Lorsque cette option est sélectionnée, la recherche DNS n'a pas lieu. 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 requis pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.</p> <p>Groupes de rôles : spécifie la liste des groupes de rôles associés à iDRAC6.</p> <p>Nom du groupe : spécifie le nom qui identifie le groupe de rôles dans Active Directory associé à iDRAC6.</p> <p>Domaine du groupe : spécifie le type de domaine du groupe dans lequel réside le groupe de rôles.</p> <p>Privilèges du groupe de rôles : spécifie le niveau des privilèges du groupe. (consultez la section Tableau 5-27)</p> <p>Ces paramètres s'affichent uniquement si iDRAC6 a été configuré en vue d'une utilisation avec un schéma Active Directory standard.</p>

Tableau 5-27. Privilèges du groupe de rôles

Paramètre	Description
Niveau de privilège du groupe de rôles	<p>Définit le privilège utilisateur iDRAC6 maximum de l'utilisateur sur l'une des options suivantes : Administrateur, Utilisateur privilégié, Utilisateur invité, Aucun ou Personnalisé.</p> <p>Consultez la section Tableau 5-28 pour connaître les droits Groupe de rôles.</p>
Ouvrir une session iDRAC6	Permet au groupe d'ouvrir une session pour accéder à iDRAC6.
Configurer iDRAC6	Permet au groupe de configurer iDRAC6.
Configurer les utilisateurs	Permet au groupe de configurer des utilisateurs.
Effacer les journaux	Permet au groupe d'effacer des journaux.
Exécuter les commandes de contrôle du serveur	Permet au groupe d'exécuter des commandes de contrôle du serveur.
Accéder à la console virtuelle	Permet au groupe d'accéder à la console virtuelle.
Accéder au média virtuel	Permet au groupe d'accéder au média virtuel.
Alertes test	Permet au groupe d'envoyer des alertes de test (e-mail et PET) à un utilisateur spécifique.
Exécuter des commandes de diagnostic	Permet au groupe d'exécuter des commandes de diagnostic.

Tableau 5-28. Droits du groupe de rôles

Propriété	Description
Administrateur	Ouvrir une session iDRAC6, Configurer iDRAC6, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du

	serveur, Accès à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic
Utilisateur privilégié	Ouvrir une session iDRAC6, Effacer les journaux, Exécuter des commandes de contrôle du serveur, Accès à la console virtuelle, Accès au média virtuel, Tester les alertes
Utilisateur invité	Ouvrir une session iDRAC6
Personnalisé	Sélectionne toute combinaison des autorisations suivantes : Ouvrir une session iDRAC6, Configurer iDRAC6, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du serveur, Accès à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic
Aucune	Aucun droit attribué

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

Sur la page de résumé Active Directory, cliquez sur **Configurer Active Directory**. La section **Certificat d'autorité de certification d'Active Directory actuel** s'affiche. Consultez [Tableau 5-29](#).

Tableau 5-29. Informations relatives au certificat d'autorité de certification d'Active Directory

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

Activation ou désactivation de l'accès à la configuration locale

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

Activation de l'accès à la configuration locale

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6 → **Réseau/Sécurité** → Services.
2. Sous **Configuration locale**, cliquez pour **décocher Désactiver les mises à jour de la configuration UTILISATEUR locale iDRAC6** pour activer l'accès.
3. Cliquez sur **Appliquer**.

Désactivation de l'accès à la configuration locale

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6 → **Réseau/Sécurité** → Services.
2. Sous **Configuration locale**, cliquez pour sélectionner **Désactiver les mises à jour de la configuration UTILISATEUR locale iDRAC6** pour désactiver l'accès.
3. Cliquez sur **Appliquer**.

Configuration des services iDRAC6

 **REMARQUE** : Pour modifier ces paramètres, vous devez disposer de l'autorisation **Configurer iDRAC6**.

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

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

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6, puis cliquez sur l'onglet **Réseau/Sécurité**.
2. Cliquez sur **Services** pour ouvrir l'écran de configuration **Services**.
3. Configurez les services suivants, si nécessaire :

- 1 Serveur Web : consultez [Tableau 5-30](#) pour accéder aux paramètres du serveur Web
- 1 SSH : consultez [Tableau 5-31](#) pour accéder aux paramètres SSH
- 1 Telnet : consultez [Tableau 5-32](#) pour accéder aux paramètres Telnet
- 1 Agent SNMP : consultez [Tableau 5-33](#) pour accéder aux paramètres de l'agent SNMP
- 1 Agent de récupération automatique du système : consultez [Tableau 5-34](#) pour accéder aux paramètres de l'agent de récupération automatique du système

4. Cliquez sur **Appliquer**.

Tableau 5-30. 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. La valeur par défaut est Cochée .
Nombre maximal de sessions	Nombre maximal de sessions simultanées du serveur Web autorisées pour ce système. Ce champ ne peut pas être modifié. Il peut y avoir 4 sessions simultanées du serveur Web.
Sessions actives	Nombre de sessions en cours sur le système, inférieur ou égal au 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 au paramètre de délai d'attente prennent effet immédiatement et réinitialisent le serveur Web. La plage du délai d'expiration est comprise entre 60 et 10 800 secondes. La valeur par défaut est 1 800 secondes.
Numéro de port HTTP	Port sur lequel iDRAC6 écoute une connexion au navigateur. 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 5-31. Paramètres SSH

Paramètre	Description
Activé	Active ou désactive SSH. Lorsqu'elle est cochée , cette case indique que SSH est activé.
Nombre maximal de sessions	Nombre maximal de sessions SSH simultanées autorisées pour ce système. Jusqu'à 4 sessions SSH simultanées sont prises en charge. Vous ne pouvez pas modifier ce champ.
Sessions actives	Nombre de sessions en cours sur le système. 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 comprise entre 60 et 10 800 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La valeur par défaut est 1 800 .
Numéro de port	Port sur lequel iDRAC6 écoute une connexion SSH. Le numéro de port par défaut est 22 .

Tableau 5-32. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Lorsqu'elle est cochée , Telnet est activé. La valeur par défaut est Décochée .
Nombre maximal de sessions	Nombre maximal de sessions Telnet simultanées autorisées pour ce système. Jusqu'à 4 sessions Telnet simultanées sont prises en charge. Vous ne pouvez pas modifier ce champ.
Sessions actives	Nombre de sessions Telnet ouvertes sur le système. Vous ne pouvez pas modifier ce champ.
Délai d'expiration	Délai d'attente en cas d'inactivité de la commande Telnet, en secondes. La plage du délai d'expiration est comprise entre 60 et 10 800 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La valeur par défaut est 1 800 .
Numéro de port	Port sur lequel iDRAC6 écoute une connexion Telnet. Le numéro de port par défaut est 23 .

Tableau 5-33. Paramètres SNMP

Paramètre	Description
Activé	Active/Désactive SNMP. Lorsqu'il est coché, SNMP est activé.
Nom de communauté SNMP	Active/Désactive le nom de communauté SNMP. Lorsqu'il est coché, le nom de la communauté SNMP est activé. Nom de communauté qui contient l'adresse IP pour la destination de l'alerte SNMP. Le nom de communauté peut contenir jusqu'à 31 caractères non blancs. La valeur par défaut est public .

Tableau 5-34. Agent de récupération de système automatique

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

Mise à jour du micrologiciel iDRAC6

-  **REMARQUE :** Si le micrologiciel iDRAC6 devient corrompu, ce qui peut être le cas si la mise à jour du micrologiciel iDRAC6 est interrompue avant la fin, vous pouvez récupérer iDRAC6 à l'aide de CMC. Consultez votre *Guide d'utilisation du micrologiciel CMC* pour obtenir des instructions.
-  **REMARQUE :** Par défaut, la mise à jour du micrologiciel conserve les paramètres iDRAC6 actuels. Lors du processus de mise à jour, vous avez la possibilité de rétablir les paramètres d'usine de la configuration iDRAC6. Si vous rétablissez les paramètres d'usine de la configuration, l'accès réseau externe sera désactivé une fois la mise à jour terminée. Vous devez activer et configurer le réseau à l'aide de l'utilitaire de configuration iDRAC6 ou via l'interface Web CMC.

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

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

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

3. Dans la section **Téléverser**, cliquez sur **Parcourir** et sélectionnez l'image de micrologiciel.

Par exemple :

```
C:\Updates\V2.2\<nom_de_l' image>.
```

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

4. Cliquez sur **Téléverser**. Le fichier va se téléverser sur iDRAC6. Cette opération peut prendre plusieurs minutes.
5. Dans l'écran **Téléverser (étape 2 sur 3)**, vous voyez les résultats de la validation effectuée sur le fichier image que vous avez téléversé.
 - 1 Si le fichier image s'est téléversé et a réussi toutes les vérifications, un message apparaît indiquant que l'image de micrologiciel a été vérifiée.
 - 1 Si l'image ne s'est pas téléversée ou n'a pas réussi les vérifications, réinitialisez iDRAC6, fermez la session actuelle, puis réessayez la mise à jour.

-  **REMARQUE :** Si vous décochez la case **Préserver la configuration**, les paramètres par défaut d'iDRAC6 sont réinitialisés. Dans les paramètres par défaut, le LAN est désactivé. Vous ne pourrez pas vous connecter à l'interface Web iDRAC6. Vous devez reconfigurer les paramètres du réseau local via l'interface Web CMC ou de la console virtuelle à l'aide de l'utilitaire de configuration iDRAC6 lors du POST du BIOS.

6. Par défaut, la case **Préserver la configuration** est **cochée** pour préserver les paramètres actuels sur iDRAC6 après une mise à niveau. Si vous ne voulez pas que les paramètres soient préservés, décochez la case **Préserver la configuration**.
7. Cliquez sur **Démarrer la mise à jour** pour démarrer le processus de mise à niveau. N'interrompez pas le processus de mise à niveau.
8. Dans la fenêtre **Téléverser (étape 3 sur 3)**, la condition de la mise à niveau est affichée. La progression de l'opération de mise à niveau de micrologiciel, indiquée en pourcentage, apparaît dans la colonne **Progression**.
9. Une fois la mise à jour du micrologiciel terminée, la fenêtre **Téléverser (étape 3 sur 3)** s'actualise avec le résultat et iDRAC6 se réinitialise automatiquement. Pour continuer à accéder à iDRAC6 via l'interface Web, fermez la fenêtre ouverte du navigateur et reconnectez-vous à iDRAC6 avec une nouvelle fenêtre de navigateur.

Mise à jour du micrologiciel iDRAC6 avec CMC

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

Vous pouvez utiliser l'interface Web CMC ou la RACADM pour mettre à jour le micrologiciel iDRAC6. Cela est possible lorsque le micrologiciel iDRAC6 est en mode Normal ou lorsqu'il est corrompu.

-  **REMARQUE :** Consultez le *Guide d'utilisation du micrologiciel Chassis Management Controller* pour obtenir des instructions relatives à l'utilisation de l'interface Web CMC.

Pour mettre à jour le micrologiciel iDRAC6, suivez les étapes suivantes :

1. Téléchargez la dernière version du micrologiciel iDRAC6 sur votre station de gestion à partir du site Web support.dell.com.
2. Ouvrez une session sur l'interface Web CMC.
3. Sélectionnez **Châssis dans l'arborescence du système**.
4. Cliquez sur l'onglet **Mise à jour**. L'écran **Mise à jour du micrologiciel** apparaît.

5. Sélectionnez un ou plusieurs iDRAC6 du même modèle à mettre à jour en cochant la case **Mettre à jour les cibles**.
6. Cliquez sur le bouton **Appliquer la mise à jour iDRAC6 Enterprise** sous la liste des composants iDRAC6.
7. Cliquez sur **Parcourir**, localisez l'image du micrologiciel iDRAC6 que vous avez téléchargée et cliquez sur **Ouvrir**.
8. Cliquez sur **Commencer la mise à jour du micrologiciel**.

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

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** → **iDRAC6**, puis cliquez sur l'onglet **Mise à jour**.
2. Cliquez sur **Restaurer**. La version actuelle et la version restaurée du micrologiciel s'affichent à la page **Restauration (étape 2 sur 3)**.
3. Cliquez sur **Suivant** pour lancer le processus de restauration du micrologiciel.

À la page **Restauration (étape 3 sur 3)**, vous verrez la condition de l'opération de restauration. Une fois la restauration du micrologiciel terminée, la page indique que l'opération s'est déroulée correctement.

Si la restauration du micrologiciel est terminée, l'iDRAC6 se réinitialise automatiquement. Pour continuer à utiliser iDRAC6 via l'interface Web, fermez la fenêtre ouverte du navigateur et reconnectez-vous à iDRAC6 avec une nouvelle fenêtre de navigateur. Un message d'erreur approprié s'affiche si une erreur se produit.

 **REMARQUE** : La fonctionnalité **Préserver la configuration** ne fonctionne pas si vous voulez restaurer le micrologiciel iDRAC6 de la version 2.2 vers la version 2.1.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation du service d'annuaire iDRAC6

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Utilisation d'iDRAC6 avec Microsoft Active Directory](#)
- [Spécifications pour l'activation de l'authentification Active Directory pour iDRAC6](#)
- [Mécanismes d'authentification Active Directory pris en charge](#)
- [Présentation d'Active Directory avec le schéma étendu](#)
- [Configuration du schéma étendu d'Active Directory pour accéder à l'iDRAC6](#)
- [Présentation d'Active Directory avec le schéma standard](#)
- [Configuration du schéma standard d'Active Directory pour accéder à iDRAC6](#)
- [Test de vos configurations](#)
- [Utilisation d'iDRAC6 avec le service d'annuaire LDAP](#)
- [Questions les plus fréquentes](#)

Un service d'annuaire 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 d'annuaire LDAP, vous pouvez le configurer pour accéder à iDRAC6, ce qui vous permet d'ajouter et de contrôler les privilèges utilisateur d'iDRAC6 pour vos utilisateurs existants au sein de votre service d'annuaire.

Utilisation d'iDRAC6 avec Microsoft Active Directory

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

Vous pouvez configurer l'authentification des utilisateurs via Microsoft Active Directory pour ouvrir une session sur iDRAC6. Vous pouvez également fournir l'autorité basée sur les rôles, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur. Pour plus d'informations, consultez les sections ultérieures.

[Tableau 6-1](#) affiche les privilèges utilisateur Active Directory iDRAC6.

Tableau 6-1. Privilèges utilisateur iDRAC6

Privilège	Description
Ouvrir une session iDRAC6	Permet à l'utilisateur d'ouvrir une session iDRAC6
Configurer iDRAC6	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 console virtuelle	Permet à l'utilisateur d'exécuter la console virtuelle
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 (e-mail et PET) à un utilisateur spécifique
Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic

Vous pouvez utiliser Active Directory pour ouvrir une session iDRAC6 via l'une des méthodes suivantes :

- 1 Interface Web
- 1 RACADM locale
- 1 Console SSH ou Telnet pour la CLI SM-CLP

La syntaxe d'ouverture de session est la même pour les trois méthodes :

```
<nom d'utilisateur@domaine>
```

ou

```
<domaine>\<nom d'utilisateur> OU <domaine>/<nom d'utilisateur>
```

où *nom d'utilisateur* est une chaîne 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, l'écran d'ouverture de session Web listera 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 d'iDRAC6 avec Microsoft Active Directory](#).

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

Pour utiliser la fonctionnalité Authentification Active Directory d'iDRAC6, vous devez déjà avoir déployé une infrastructure Active Directory. Consultez le site Web 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 devrez également activer le protocole SSL (Secure Socket Layer) sur tous les contrôleurs de domaine auxquels se connecte l'iDRAC6. Pour des informations plus spécifiques, consultez [Activation de SSL sur un contrôleur de domaine](#).

Activation de SSL sur un contrôleur de domaine

Lorsqu'iDRAC6 authentifie les utilisateurs par rapport à un contrôleur de domaine d'Active Directory, il démarre une session SSL avec le contrôleur de domaine. À ce moment, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (AC), dont le certificat racine est également téléversé sur iDRAC6. En d'autres termes, pour que l'iDRAC6 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'autorité de certification 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-droite 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'autorité de certification 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-droite sur le certificat d'autorité de certification 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](#) sur iDRAC6.

Pour télécharger le certificat à l'aide de la RACADM, consultez [Configuration d'Active Directory avec le schéma standard via la RACADM](#).

Pour télécharger le certificat via l'interface Web, consultez [Configuration d'Active Directory avec le schéma standard via 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 télécharger le certificat du serveur iDRAC6 sur le contrôleur de domaine d'Active Directory. Cette étape supplémentaire n'est pas nécessaire si Active Directory ne procède pas à l'authentification du client lors de la phase d'initialisation d'une session SSL.

Utilisez la procédure suivante pour importer le certificat SSL du micrologiciel iDRAC6 dans toutes les listes de certificats 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 autorité de certification connue et le certificat de cette dernière 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 iDRAC6 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-droite 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 d'iDRAC6 dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

Si vous avez installé votre propre certificat, assurez-vous que l'AC qui signe votre certificat figure 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**.

Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès de l'utilisateur sur iDRAC6 au moyen de deux méthodes : vous pouvez utiliser la solution *schéma étendu*, que Dell a personnalisée pour y ajouter des objets Active Directory définis par Dell, ou vous pouvez utiliser la solution *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 :

- 1 Tous les objets de contrôle d'accès sont maintenus dans Active Directory.
- 1 Flexibilité maximale lors de la configuration de l'accès des utilisateurs sur différentes cartes iDRAC6 avec différents niveaux de privilèges.

La solution de schéma standard comporte l'avantage suivant : aucune extension de schéma n'est requise, 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.

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 d'annuaire.

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

Présentation des extensions de schéma d'iDRAC6

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

Présentation des objets Active Directory

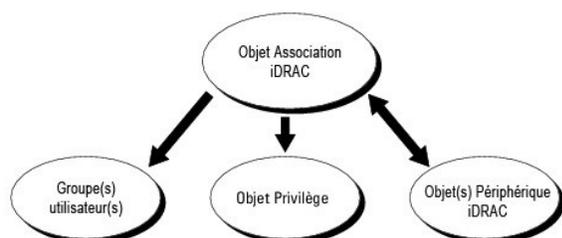
Pour chacun des périphériques iDRAC6 physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, vous devez créer au moins un objet Association et un objet Périphérique iDRAC6. Vous pouvez créer plusieurs objets Association et chaque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

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

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

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

Figure 6-1. Configuration 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 iDRAC6 pour chaque périphérique iDRAC6 du réseau que vous voulez intégrer à Active Directory pour en gérer l'authentification et l'autorisation avec iDRAC6.

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

L'extension Dell sur le snap-in ADUC MMC permet seulement l'association de l'objet Privilège et des objets iDRAC6 du même domaine avec l'objet Association. L'extension Dell ne permet pas l'ajout d'un groupe ou d'un objet iDRAC6 d'autres domaines en tant que membre produit de l'objet Association.

Lorsque vous ajoutez des groupes universels à partir de domaines séparés, créez un objet Association avec une étendue universelle. Les objets Association par défaut créés par l'utilitaire Dell Schema Extender sont des groupes locaux de domaines et ne fonctionnent pas avec les groupes universels d'autres domaines.

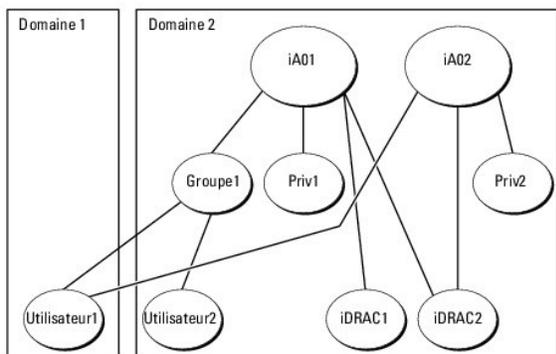
Les utilisateurs, groupes d'utilisateurs ou groupes d'utilisateurs imbriqués depuis tout domaine peuvent être ajoutés dans l'objet Association. Les solutions de schéma étendu prennent en charge tout type de groupe d'utilisateurs et toute imbrication de groupes d'utilisateurs à travers plusieurs domaines 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.

[Figure 6-2](#) fournit un exemple d'accumulation de privilèges à l'aide du schéma étendu.

Figure 6-2. Accumulation de privilèges pour un utilisateur



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

Par exemple, Priv1 possède les privilèges Ouvrir une session, Média virtuel et Effacer les journaux, et Priv2 a les privilèges Ouvrir une session iDRAC, Configurer iDRAC et Tester les alertes. Par conséquent, Utilisateur1 a désormais l'ensemble des privilèges Ouvrir une session iDRAC, Média virtuel, Effacer les journaux, Configurer iDRAC et Tester les alertes, correspondant 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 uniquement les privilèges Priv1 sur iDRAC1. Utilisateur2 possède les privilèges Priv1 sur iDRAC1 et iDRAC2. En outre, cette figure illustre que l'utilisateur1 peut être dans un domaine différent et peut être un membre d'un groupe.

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

Pour pouvoir utiliser Active Directory pour accéder à iDRAC6, configurez le logiciel Active Directory et iDRAC6 en suivant 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 Active Directory](#)).
3. Ajoutez des utilisateurs iDRAC6 et leurs privilèges à Active Directory (consultez [Ajout d'utilisateurs iDRAC6 et de leurs privilèges à Active Directory](#)).
4. Configurez les propriétés Active Directory d'iDRAC6 avec l'interface Web d'iDRAC6 ou la RACADM (consultez [Configuration de Microsoft Active Directory avec le schéma étendu via l'interface Web iDRAC6](#) ou [Configuration d'Active Directory avec le schéma étendu via la RACADM](#)).

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 : Étendre le nouveau schéma ou installer la nouvelle extension sur le snap-in Utilisateurs et ordinateurs Active Directory n'a aucun impact sur les versions précédentes de ce produit.

L'extension de schéma et l'extension snap-in MMC Utilisateurs et ordinateurs Active Directory sont disponibles sur le DVD *Dell Systems Management Tools and Documentation*. Pour des informations sur l'installation, consultez [Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory](#). Pour des détails complémentaires sur l'extension du schéma pour iDRAC6 et sur l'installation du snap-in MMC Utilisateurs et ordinateurs Active Directory, 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 iDRAC6 ou des objets Périphérique iDRAC6, sélectionnez **Objet avancé Gestion à distance Dell**.

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 l'une des méthodes suivantes :

1. l'utilitaire Dell Schema Extender ;
1. 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 :

- 1 Lecteur DVD : \SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- 1 <LecteurDVD >:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender

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

⚠ PRÉCAUTIONS : 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 :

- 1 Classes (consultez [Tableau 6-2](#) à [Tableau 6-7](#))
- 1 Attributs ([Tableau 6-8](#))

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

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

Nom de classe	Numéro d'identification d'objet (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 6-3. Classe dellRacDevice

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

Tableau 6-4. Classe dellIDRACAssociationObject

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

Tableau 6-5. Classe dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Définit les privilèges (droits d'autorisation) pour iDRAC6
Type de classe	Classe auxiliaire
SuperClasses	Aucune
Attributs	dell sLoginUser dell sCardConfigAdmin dell sUserConfigAdmin dell sLogClearAdmin dell sServerResetUser dell sConsoleRedirectUser dell sVirtualMediaUser dell sTestAlertUser dell sDebugCommandAdmin

Tableau 6-6. Classe dellPrivileges

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

Tableau 6-7. Classe dellProduct

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

Tableau 6-8. Liste des attributs ajoutés au schéma Active Directory

Nom/Description de l'attribut	OID attribué/Identifiant d'objet de syntaxe	Valeur unique
dellPrivilegeMember Liste des objets dellPrivilege qui appartiennent à cet attribut.	1.2.840.113556.1.8000.1280.1.1.2.1 Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Liste des objets dellRacDevice et DellDRACDevice qui appartiennent à ce rôle. Cet attribut est le lien vers l'avant vers le lien vers l'arrière dellAssociationMembers. ID de lien : 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dell sLoginUser TRUE si l'utilisateur a les droits Ouvrir une session sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.3 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dell sCardConfigAdmin TRUE si l'utilisateur a les droits Configuration de carte sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.4 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dell sUserConfigAdmin TRUE si l'utilisateur a les droits Configuration utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dell sLogClearAdmin TRUE si l'utilisateur a les droits Effacement de journal sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.6 Booléen (LDAPTYPE_BOOLEAN	TRUE

	1.3.6.1.4.1.1466.115.121.1.7)	
dellServerResetUser TRUE si l'utilisateur a les droits Réinitialisation de serveur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.7 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellConsoleRedirectUser TRUE si l'utilisateur a les droits Console virtuelle sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.8 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellVirtualMediaUser TRUE si l'utilisateur a les droits Média virtuel sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.9 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellTestAlertUser TRUE si l'utilisateur a les droits Utilisateur et test d'alertes sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellDebugCommandAdmin 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 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La version de schéma actuelle est utilisée pour mettre à jour le schéma.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Cet attribut est le type 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 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut lié dellProductMembers. ID de lien : 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nom unique (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs Active Directory pour que l'administrateur puisse gérer les périphériques iDRAC6, les utilisateurs et les groupes d'utilisateurs, les associations iDRAC6 et les privilèges iDRAC6.

Lorsque vous installez votre logiciel Systems Management Software à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez étendre le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** pendant la procédure d'installation. Consultez le *Guide d'installation rapide du logiciel Dell OpenManage* pour des instructions supplémentaires sur l'installation du logiciel Systems Management Software. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du snap-in se trouve dans :

<lecteur DVD>:\SYSTEMGMT\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 iDRAC6 d'Active Directory. Si vous n'installez pas le pack administrateur, vous ne pouvez pas visualiser l'objet iDRAC6 Dell dans le conteneur.

Consultez la section [Ouverture du snap-in Utilisateurs et ordinateurs Active Directory](#) pour plus d'informations.

Ouverture du snap-in Utilisateurs et ordinateurs Active Directory

Pour ouvrir le snap-in Utilisateurs et ordinateurs Active Directory :

1. Si vous êtes connecté au contrôleur de domaine, cliquez sur **Démarrer Outils d'administration** → **Utilisateurs et ordinateurs Active Directory**.

Si vous n'avez pas ouvert une session sur le contrôleur de domaine, la version appropriée du pack administrateur Microsoft doit être installée sur votre système local. Pour installer ce pack administrateur, cliquez sur **Démarrer** → **Exécuter**, tapez MMC et appuyez sur **Entrée**.

La MMC apparaît.

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 iDRAC6 et de leurs privilèges à Active Directory

Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous permet d'ajouter des utilisateurs iDRAC6 et des privilèges en créant des objets iDRAC6, Association et Privilège. Pour ajouter chaque type d'objet, effectuez les procédures suivantes :

- 1 Créez un objet Périphérique iDRAC6
- 1 Créer un objet Privilège
- 1 Créer un objet Association
- 1 Ajoutez des objets à un objet Association

Création d'un objet Périphérique iDRAC6

1. Dans la fenêtre **Racine de la console MMC**, cliquez-droite sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet avancé Gestion à distance Dell**.
La fenêtre **Nouvel objet** apparaît.
3. Entrez un nom pour le nouvel objet. Le nom doit être identique au nom iDRAC6 que vous saisissez à l'étape A de [Configuration de Microsoft Active Directory avec le schéma étendu via l'interface Web iDRAC6](#).
4. Sélectionnez l'objet Périphérique iDRAC6.
5. Cliquez sur **OK**.

Création d'un objet Privilège

 **REMARQUE :** Un objet Privilège doit être créé dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console (MMC)**, cliquez-droite sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet avancé Gestion à distance Dell**.
La fenêtre **Nouvel objet** apparaît.
3. Entrez un nom pour le nouvel objet.
4. Sélectionnez **Objet Privilège**.
5. Cliquez sur **OK**.
6. Cliquez-droite sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
7. Cliquez sur l'onglet **Privilèges de gestion à distance** et sélectionnez les privilèges à attribuer à l'utilisateur ou au groupe (consultez [Tableau 5-14](#)).

Création d'un objet Association

 **REMARQUE :** L'objet Association iDRAC6 est dérivé d'un groupe et son étendue est définie sur Domaine local.

1. Dans la fenêtre **Racine de la console (MMC)**, cliquez-droite sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet avancé Gestion à distance Dell**.
Cette action ouvre la fenêtre **Nouvel objet**.
3. Entrez un nom pour le nouvel objet.

4. Sélectionnez **Objet Association**.
5. Sélectionnez l'étendue de l'objet **Association**.
6. Cliquez sur **OK**.
7. Fournissez des privilèges d'accès aux utilisateurs authentifiés afin de leur permettre d'accéder aux objets **Association** créés. Pour ce faire :
 - a. Accédez à **Outils d'administration** → **Modification ADSI**. La fenêtre **Modification ADSI** s'affiche.
 - b. Dans le volet droit, naviguez vers l'objet **Association** créé, cliquez- droite et sélectionnez **Propriétés**.
 - c. Dans l'onglet **Sécurité**, cliquez sur **Ajouter**.
 - d. Saisissez **Authenticated Users**, cliquez sur **Vérifier les noms**, puis sur **OK**. Les **Utilisateurs authentifiés** sont ajoutés à la liste des **Groupes et noms d'utilisateur**.
 - e. Cliquez sur **OK**.

Ajout d'objets à un objet **Association**

En utilisant la fenêtre **Propriétés de l'objet Association**, vous pouvez associer des utilisateurs, des groupes d'utilisateurs, des objets **Privilège** et des périphériques **iDRAC6** ou des groupes de périphériques **iDRAC6**.

Vous pouvez ajouter des groupes d'utilisateurs et des périphériques **iDRAC6**. La procédure de création de groupes associés à **Dell** et de groupes non associés à **Dell** est identique.

Ajout d'utilisateurs ou de groupes d'utilisateurs

1. Cliquez-droite sur l'objet **Association** et sélectionnez **Propriétés**.
2. Sélectionnez l'onglet **Utilisateurs** et cliquez sur **Ajouter**.
3. Entrez le nom de l'utilisateur ou du groupe d'utilisateurs et cliquez sur **OK**.

Ajout de privilèges

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Entrez le nom de l'objet **Privilège** et cliquez sur **OK**.

Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet **Privilège** à l'association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs durant l'authentification auprès d'un périphérique **iDRAC6**. Vous ne pouvez ajouter qu'un seul objet **Privilège** à un objet **Association**.

Ajout de périphériques **iDRAC6** ou de groupes de périphériques **iDRAC6**

Pour ajouter des périphériques **iDRAC6** ou des groupes de périphériques **iDRAC6** :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Entrez le nom des périphériques **iDRAC6** ou des groupes de périphériques **iDRAC6**, puis cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

Cliquez sur l'onglet **Produits** pour ajouter un périphérique **iDRAC6** connecté au réseau qui est disponible pour les utilisateurs ou groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques **iDRAC6** à un objet **Association**.

Configuration de Microsoft Active Directory avec le schéma étendu via 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. Dans l'arborescence du système, sélectionnez **Système** → **Accès à distance** → **iDRAC6** → Onglet **Réseau/Sécurité** → **Service d'annuaire** → **Microsoft Active Directory**.

L'écran de résumé Active Directory apparaît.

4. Faites défiler jusqu'au bas de l'écran, puis cliquez sur **Configurer Active Directory**.

L'écran **Étape 1 sur 4 Active Directory** apparaît.

5. Pour valider le certificat SSL de vos serveurs Active Directory, cochez la case **Validation des certificats activée** sous **Paramètres des certificats**.

Si vous ne souhaitez pas valider le certificat SSL de vos serveurs Active Directory, passez à l'étape 7.

6. Sous **Téléverser le certificat d'autorité de certification d'Active Directory**, entrez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat, puis cliquez sur **Téléverser**.

 **REMARQUE** : Vous devez saisir le chemin de fichier absolu qui comprend le chemin et le nom de fichier complets ainsi que l'extension du fichier.

Les informations relatives au certificat d'autorité de certification d'Active Directory que vous avez téléversé s'affichent dans la section **Certificat d'autorité de certification d'Active Directory actuel**.

7. Cliquez sur **Suivant**.

L'écran **Étape 2 sur 4 Configuration et gestion d'Active Directory** apparaît.

8. Cochez la case **Active Directory activé**.

 **REMARQUE** : Dans cette version, la fonctionnalité Authentification bifactorielle (TFA) par carte à puce n'est pas prise en charge si Active Directory est configuré pour le schéma étendu. La fonctionnalité Connexion directe (SSO) est prise en charge à la fois pour le schéma standard et pour le schéma étendu.

9. Cliquez sur **Ajouter** pour entrer le **nom de domaine utilisateur**. Entrez le nom de domaine dans le champ de texte, 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 entrer le nom d'utilisateur.

10. Dans le champ **Délai d'attente**, entrez le nombre de secondes devant s'écouler avant qu'iDRAC6 puisse obtenir les réponses d'Active Directory.

11. Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Si elle est déjà configurée, les **Adresses 1 à 3 des serveurs des contrôleurs de domaine** sont ignorées. Sélectionnez **Domaine utilisateur de connexion** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Sinon, sélectionnez **Définir un domaine** et saisissez le nom de domaine à utiliser pour 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, ces adresses sont celles des contrôleurs de domaine dans lesquels l'objet Périphérique iDRAC6 et les objets Association sont situés. Si **Schéma standard** est sélectionné, les contrôleurs de domaine sont ceux où se trouvent les comptes d'utilisateur et les groupes de rôles.

 **REMARQUE** : iDRAC6 ne bascule pas vers les contrôleurs de domaine spécifiés lorsque la recherche DNS échoue ou lorsque aucun des serveurs renvoyés par la recherche DNS ne fonctionne.

12. Sélectionnez l'option **Définir des adresses de contrôleur de domaine** pour autoriser iDRAC6 à utiliser les adresses des serveurs des contrôleurs de domaine Active Directory qui sont spécifiées. La recherche DNS n'est pas effectuée. Spécifiez l'adresse IP ou le nom de domaine complet des contrôleurs de domaine. Lorsque l'option **Définir des adresses de contrôleur de domaine** est sélectionnée, au moins 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, ces adresses sont celles des contrôleurs de domaine dans lesquelles l'objet Périphérique iDRAC6 et les objets Association sont situés.

 **REMARQUE** : Le nom de domaine complet ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ **Sujet** ou **Nom alternatif du sujet** de votre certificat du contrôleur de domaine si la validation des certificats est activée.

13. Cliquez sur **Suivant**.

L'écran **Étape 3 sur 4 Configuration et gestion d'Active Directory** apparaît.

14. Sous **Sélection du schéma**, cochez la case **Sélection d'un schéma étendu**.

15. Cliquez sur **Suivant**.

L'écran **Étape 4 sur 4 Active Directory** apparaît.

16. Sous **Paramètres du schéma étendu**, entrez le **nom iDRAC6** et le **nom de domaine iDRAC6** pour configurer l'objet Périphérique iDRAC6 et son emplacement dans Active Directory.

17. Cliquez sur **Terminer** pour sauvegarder vos modifications, puis sur **Terminé**.

La page résumé **Configuration et gestion d'Active Directory** apparaît. Testez ensuite les paramètres Active Directory que vous venez de configurer.

18. Faites défiler jusqu'au bas de l'écran, puis cliquez sur **Paramètres du test**.

L'écran **Paramètres du test Active Directory** apparaît.

19. Entrez vos nom d'utilisateur et mot de passe iDRAC6, puis cliquez sur **Démarrer le test**.

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 iDRAC6 pour prendre en charge l'ouverture de session Active Directory. Naviguez jusqu'à l'écran **Réseau** (cliquez sur **Système** → **Accès à distance** → iDRAC6, puis cliquez sur **Réseau/Sécurité** → onglet **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 d'Active Directory avec le schéma étendu via la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory iDRAC6 avec le schéma étendu via l'interface de ligne de commande (CLI) RACADM au lieu de l'interface Web.

1. Ouvrez une invite de commande et entrez les commandes RACADM suivantes :

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

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

racadm config -g cfgActiveDirectory -o cfgADRacDomain <nom de domaine pleinement qualifié du rac>

racadm config -g cfgActiveDirectory -o cfgADDomainController1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o cfgADDomainController2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o cfgADDomainController3 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
```

 **REMARQUE :** Vous devez configurer au moins une des trois adresses. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Avec le schéma étendu, il s'agit des noms de domaine pleinement qualifiés ou adresses IP des contrôleurs de domaine où ce périphérique iDRAC6 est situé. En mode Schéma étendu, les serveurs de catalogue global ne sont pas du tout utilisés.

Pour désactiver la validation des certificats durant l'établissement de liaisons SSL, entrez 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 activer la validation des certificats durant l'établissement de liaisons SSL, entrez 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 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 nom DNS fourni par le serveur DHCP, entrez la commande RACADM suivante :

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. Si le DHCP est désactivé sur iDRAC6 ou si vous voulez entrer manuellement votre adresse IP DNS, entrez 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 d'entrer le nom d'utilisateur durant l'ouverture de session sur l'interface Web iDRAC6, entrez la commande suivante :

```
racadm config -g cfgUserDomain -o cfgUserDomainName <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine> -i
<index>
```

Vous pouvez configurer jusqu'à 40 domaines utilisateur avec des numéros d'index compris entre 1 et 40.

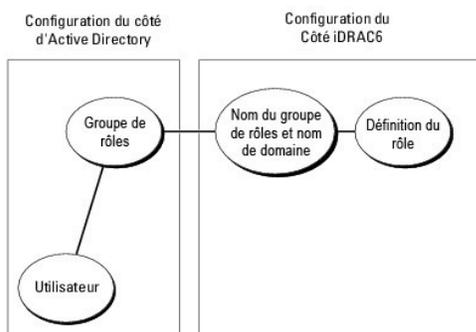
Consultez [Utilisation d'iDRAC6 avec Microsoft Active Directory](#) pour obtenir des détails sur les domaines utilisateur.

- 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 [Figure 6-3](#), l'utilisation du schéma standard pour l'intégration d'Active Directory nécessite une configuration sur Active Directory et sur l'iDRAC6.

Figure 6-3. Configuration de l'iDRAC6 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 une carte iDRAC6 spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cette carte iDRAC6. Contrairement à la solution du schéma étendu, le niveau des rôles et des privilèges est défini sur chaque carte iDRAC6 et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque iDRAC6. [Tableau 6-9](#) affiche les privilèges par défaut des groupes de rôles.

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

Groupes de rôles	Niveau de privilège par défaut	Droits accordés	Masque binaire
Groupe de rôles 1	Aucune	Ouvrir une session iDRAC, Configurer iDRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du serveur, Accès à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic	0x000001ff
Groupe de rôles 2	Aucune	Ouvrir une session iDRAC, Configurer iDRAC, Exécuter des commandes de contrôle du serveur, Accès à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic	0x000000f9
Groupe de rôles 3	Aucune	Ouvrir une session iDRAC	0x00000001
Groupe de rôles 4	Aucune	Aucun droit attribué	0x00000000
Groupe de rôles 5	Aucune	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 d'Active Directory pour accéder à iDRAC6

Vous devez suivre les étapes suivantes pour configurer Active Directory pour qu'un utilisateur Active Directory puisse accéder à iDRAC6 :

- Sur un serveur Active Directory (contrôleur de domaine), ouvrez le **snap-in Utilisateurs et ordinateurs Active Directory**.
- Créez un groupe ou sélectionnez un groupe existant. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse

accéder à iDRAC6.

3. Configurez le nom du groupe et le nom du domaine sur iDRAC6 en utilisant l'interface Web ou la RACADM (consultez [Configuration d'Active Directory avec le schéma standard via l'interface Web iDRAC6](#) ou [Configuration d'Active Directory avec le schéma standard via la RACADM](#)).

Configuration d'Active Directory avec le schéma standard via 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. Dans l'arborescence du système, sélectionnez **Système** → **Accès à distance** → iDRAC6 → Onglet **Réseau/Sécurité** → **Service d'annuaire** → **Microsoft Active Directory**.

La page de résumé Active Directory apparaît.

4. Faites défiler jusqu'au bas de l'écran, puis cliquez sur **Configurer Active Directory**.

L'écran **Étape 1 sur 4 Active Directory** apparaît.

5. Sous **Paramètres des certificats**, sélectionnez **Validation des certificats activée**.
6. Sous **Téléverser le certificat d'autorité de certification d'Active Directory**, entrez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat, puis cliquez sur **Téléverser**.

 **REMARQUE** : Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

Les informations relatives au certificat d'autorité de certification d'Active Directory que vous avez téléversé s'affichent dans la section **Certificat d'autorité de certification d'Active Directory actuel**.

7. Cliquez sur **Suivant**.

L'écran **Étape 2 sur 4 Configuration et gestion d'Active Directory** apparaît.

8. Cochez la case **Active Directory activé**.
9. Sélectionnez **Activer la connexion par carte à puce** pour activer l'ouverture de session par carte à puce. Vous serez invité à ouvrir une session par carte à puce lors de chaque tentative ultérieure d'ouverture de session via l'interface utilisateur graphique.
10. Sélectionnez **Activer la connexion directe** si vous souhaitez ouvrir une session iDRAC6 sans entrer vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe.
11. Cliquez sur **Ajouter** pour entrer le **nom de domaine utilisateur**. Entrez le nom de domaine dans le champ de texte, 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 entrer le nom d'utilisateur.
12. Dans le champ **Délai d'attente**, entrez le nombre de secondes devant s'écouler avant qu'iDRAC6 puisse obtenir les réponses d'Active Directory.
13. Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Si elle est déjà configurée, les **Adresses 1 à 3 des serveurs des contrôleurs de domaine** sont ignorées. Sélectionnez **Domaine utilisateur de connexion** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Sinon, sélectionnez **Définir un domaine** et saisissez le nom de domaine à utiliser pour 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.
14. Sélectionnez l'option **Définir des adresses de contrôleur de domaine** pour autoriser iDRAC6 à utiliser les adresses des serveurs des contrôleurs de domaine Active Directory qui sont spécifiées. La recherche DNS n'est pas effectuée. Spécifiez l'adresse IP ou le nom de domaine complet des contrôleurs de domaine. Lorsque l'option **Définir des adresses de contrôleur de domaine** est sélectionnée, au moins 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** : iDRAC6 ne bascule pas vers les contrôleurs de domaine spécifiés lorsque la recherche DNS échoue ou lorsque aucun des serveurs renvoyés par la recherche DNS ne fonctionne.

15. Cliquez sur **Suivant**.

L'écran **Étape 3 sur 4 Configuration et gestion d'Active Directory** apparaît.

16. Sous **Sélection du schéma**, cochez la case **Sélection d'un schéma standard**.
17. Cliquez sur **Suivant**.

L'écran **Étape 4a sur 4 Active Directory** apparaît.

18. Sous **Paramètres du schéma standard**, sélectionnez l'option **Rechercher des serveurs de catalogue global avec DNS** et saisissez le **Nom de domaine racine** à utiliser lors d'une recherche DNS pour obtenir les serveurs de catalogue global Active Directory. Si l'option est déjà configurée, les Adresses 1 à 3 des serveurs 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.

 **REMARQUE** : iDRAC6 ne bascule pas vers les serveurs de catalogue global spécifiés lorsque la recherche DNS échoue ou lorsque aucun des serveurs renvoyés par la recherche DNS ne fonctionne.

19. Sélectionnez l'option **Définir des adresses de 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 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.

 **REMARQUE** : Le serveur de catalogue global est requis uniquement pour le schéma standard lorsque les comptes d'utilisateur et les groupes de rôles sont dans des domaines différents. De plus, dans ce scénario à plusieurs domaines, seul le groupe universel peut être utilisé. Si vous utilisez l'interface utilisateur Web iDRAC6 pour configurer Active Directory, vous devez entrer une adresse globale même si l'utilisateur et le groupe proviennent du même domaine.

20. Cliquez sur un bouton **Groupe de rôles** pour ajouter un groupe de rôles.

L'écran **Étape 4b sur 4 Configurer le groupe de rôles** apparaît.

21. Entrez le **Nom du groupe**. Le nom du groupe identifie le groupe de rôles d'Active Directory associé à iDRAC6.
22. Entrez le **Domaine du groupe**. Le **Domaine du groupe** est le nom de domaine racine pleinement qualifié de la forêt.
23. Dans la section **Privilèges du groupe de rôles**, définissez les privilèges du groupe. Consultez [Tableau 5-14](#) pour plus d'informations sur les privilèges des groupes de rôles.

 **REMARQUE** : Si vous modifiez des droits, le privilège du groupe de rôles actuel (Administrateur, Utilisateur privilégié ou Utilisateur invité) devient celui d'un groupe personnalisé ou un privilège de groupe de rôles correspondant aux droits modifiés.

24. Cliquez sur **OK** pour enregistrer les paramètres Groupe de rôles.

Une boîte de dialogue d'alerte s'affiche, indiquant que vos paramètres ont été modifiés. Cliquez sur **OK** pour revenir à l'écran **Étape 4a sur 4 Configuration et gestion d'Active Directory**.

25. Pour ajouter un groupe de rôles supplémentaire, répétez les étapes [étape 20](#) à [étape 24](#).

26. Cliquez sur **Terminer**, puis sur **Terminé**.

L'écran résumé principal **Configuration et gestion d'Active Directory** apparaît. Testez les paramètres Active Directory que vous venez de configurer.

27. Faites défiler jusqu'au bas de l'écran, puis cliquez sur **Paramètres du test**.

L'écran **Paramètres de test Active Directory** apparaît.

28. Entrez vos nom d'utilisateur et mot de passe iDRAC6, puis cliquez sur **Démarrer le test**.

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 iDRAC6 pour prendre en charge l'ouverture de session Active Directory. Naviguez jusqu'à l'écran **Réseau** (cliquez sur **Système** → **Accès à distance** → **iDRAC6**, puis cliquez sur **Réseau/Sécurité** → onglet **Réseau**) pour configurer manuellement le(s) serveur(s) DNS ou utiliser DHCP pour obtenir le(s) serveurs DNS.

Vous avez terminé la configuration d'Active Directory avec le schéma standard.

Configuration d'Active Directory avec le schéma standard via la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory d'iDRAC6 avec le schéma standard via la CLI RACADM au lieu de l'interface Web.

1. Ouvrez une invite de commande et entrez les commandes RACADM suivantes :

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 2

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

```
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupDomain <nom de domaine pleinement qualifié>
```

```
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <valeur du masque binaire pour
des droits de groupe de rôles spécifiques>
```

 **REMARQUE :** Pour des valeurs du masque binaire pour des droits de groupe de rôles spécifiques, consultez [Tableau 6-9](#).

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
```

 **REMARQUE :** Entrez le nom de domaine complet du contrôleur de domaine *et non* le nom de domaine complet du domaine. Par exemple, entrez `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 est uniquement nécessaire pour le schéma standard lorsque les comptes d'utilisateur et les groupes de rôles sont dans des domaines différents. De plus, dans ce scénario à plusieurs domaines, seul le groupe universel peut être utilisé.

 **REMARQUE :** Le nom de domaine complet ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ **Sujet** ou **Nom alternatif** du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.

Pour désactiver la validation des certificats durant l'établissement de liaisons SSL, entrez 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 activer la validation des certificats durant l'établissement de liaisons SSL, entrez 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 nom DNS fourni par le serveur DHCP, entrez les commandes RACADM suivantes :

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. Si le protocole DHCP est désactivé sur iDRAC6 ou que vous voulez entrer manuellement l'adresse IP DNS, entrez les commandes RACADM suivantes :

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP de DNS principale>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP de DNS secondaire>
```

4. Si vous souhaitez configurer une liste de domaines utilisateur afin de devoir seulement entrer le nom d'utilisateur lors de l'ouverture de session via l'interface Web, entrez la commande suivante :

```
racadm config -g cfgUserDomain -o cfgUserDomainName <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine> -i
<index>
```

Jusqu'à 40 domaines utilisateur peuvent être configurés avec des numéros d'index compris entre 1 et 40.

Consultez [Utilisation d'iDRAC6 avec Microsoft Active Directory](#) pour obtenir des détails sur les domaines utilisateur.

Test de vos configurations

Pour vérifier si votre configuration fonctionne, ou si vous devez 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 du test** au bas de l'écran. 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 l'écran 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](#).

Si vous devez apporter des modifications à vos paramètres, cliquez sur l'onglet **Active Directory**, puis modifiez la configuration pas à pas.

Utilisation d'iDRAC6 avec le service d'annuaire LDAP

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 d'annuaire.

Pour rendre l'implémentation LDAP iDRAC6 générique, la similitude entre les différents services d'annuaire est utilisée pour grouper les utilisateurs, puis pour adresser la relation utilisateur-groupe. Le schéma constitue l'action spécifique au service d'annuaire. 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 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 de l'interface utilisateur affiche uniquement Cet iDRAC dans le menu déroulant.

 **REMARQUE :** Dans cette version, seuls les services d'annuaire basé sur openLDAP et sur openDS sont pris en charge. Les caractères « < » et « > » ne sont pas autorisés dans le nom d'utilisateur pour openLDAP ni pour OpenDS.

Configuration du service d'annuaire LDAP générique via 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 **Système** et cliquez sur **Accès à distance** → iDRAC6 → **Onglet Réseau/Sécurité** → **Service d'annuaire** → **Service d'annuaire LDAP générique**.
4. La page **Configuration et gestion LDAP génériques** affiche les paramètres LDAP générique iDRAC6 actuels. Faites défiler vers le bas de la page **Configuration et gestion LDAP génériques** et cliquez sur **Configuration 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 LDAP génériques** 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.

5. Sous **Paramètres du certificat**, cochez **Activer la validation de certificats** pour activer la validation du 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.

 **PRÉCAUTIONS :** 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 **CN du certificat du serveur doit correspondre à l'adresse du serveur LDAP** dans iDRAC6 pour que la validation du certificat soit fiable.

6. Sous **Téléverser le certificat d'autorité de certification du service d'annuaire**, 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.

7. Cliquez sur **Téléverser**.

Le certificat de l'autorité de certification racine qui signe tous les certificats de serveurs SSL (Security Socket Layer) des contrôleurs de domaine sera téléversé.

8. Cliquez sur **Suivant** pour accéder à la page **Étape 2 sur 3 Configuration et gestion LDAP génériques**. 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 par carte à puce (TFA) et Connexion directe (SSO) ne sont pas prises en charge pour le service d'annuaire LDAP générique.
9. Sélectionnez **Activer le protocole 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.
10. Sélectionnez l'option **Utiliser le nom unique pour rechercher l'appartenance au groupe** afin d'utiliser le nom unique comme 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.
11. Dans le champ **Adresse du serveur LDAP**, saisissez le nom de domaine complet 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.
12. Saisissez le port utilisé pour LDAP sur SSL dans le champ **Port du serveur LDAP**. Le port par défaut est 636.
13. 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.
14. 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.
15. 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 débiter.
16. Dans le champ **Attribut de la connexion 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.
17. 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*.
18. 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.
19. Cliquez sur **Suivant** pour accéder à la page **Étape 3a sur 3 Configuration et gestion LDAP génériques**. 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.
20. Sous **Groupes de rôles**, cliquez sur un **Groupe de rôles**.

La page **Étape 3b sur 3 Configuration et gestion LDAP génériques** apparaît. Utilisez cette page pour configurer chaque groupe de rôles utilisé pour contrôler la règle d'autorisation applicable aux utilisateurs.
21. Saisissez le **nom unique (DN) du groupe** qui identifie le groupe de rôles au sein du service d'annuaire LDAP générique associé à iDRAC6.
22. Dans la section **Privilèges de groupe de rôles**, spécifiez les privilèges associés au groupe en sélectionnant le **niveau de privilèges du groupe de rôles**. Par exemple, si vous sélectionnez **Administrateur**, tous les privilèges sont sélectionnés pour ce niveau de droit.
23. 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 LDAP génériques** qui affiche vos paramètres Groupes de rôles.
24. Configurez des groupes de rôles supplémentaires, le cas échéant.
25. Cliquez sur **Terminer** pour retourner à la page de résumé **Configuration et gestion LDAP génériques**.
26. Cliquez sur **Paramètres du test** pour vérifier les paramètres LDAP générique.
27. 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 de la connexion utilisateur* utilisé et le nom d'utilisateur saisi doit correspondre à la valeur de l'attribut choisi.

 **REMARQUE** : Lors du test des paramètres LDAP avec l'option **Activer la validation de certificats** cochée, iDRAC6 requiert l'identification du serveur LDAP par le nom de domaine complet, et non par une adresse IP. Si le serveur LDAP est identifié par une adresse IP, la validation du certificat échoue, car iDRAC6 n'est pas en mesure de communiquer avec le serveur LDAP.

Les résultats du test et le journal du test sont affichés. Vous avez terminé la configuration du service d'annuaire LDAP générique.

Questions les plus fréquentes

Problèmes d'ouverture de session via Active Directory

L'ouverture d'une session iDRAC6 par connexion directe Active Directory prend presque 4 minutes.

L'ouverture de session normale par connexion directe Active Directory nécessite généralement moins de 10 secondes, mais l'ouverture de session sur iDRAC6 avec la connexion directe Active Directory peut prendre presque 4 minutes si vous avez spécifié **Serveur DNS préféré** et **Serveur DNS auxiliaire** dans la page **Réseau** iDRAC6 et qu'une panne du serveur DNS préféré est survenue. Des expirations du délai d'attente DNS peuvent se produire lorsque le serveur DNS est en panne. iDRAC6 vous connecte à l'aide du serveur DNS auxiliaire.

J'ai configuré Active Directory pour un domaine présent dans Windows Server 2008 Active Directory et j'ai effectué ces configurations. Un domaine enfant ou un sous- domaine est présent pour le domaine, l'utilisateur et le groupe sont présents dans le même domaine enfant, et l'utilisateur est un membre de ce groupe. Lorsque j'essaie à présent de me connecter à iDRAC6 avec l'utilisateur présent dans ce domaine enfant, la connexion directe Active Directory échoue.

Le type de groupe est peut-être incorrect. Le serveur Active Directory possède deux sortes de types de groupe :

- 1 **Sécurité** - les groupes de sécurité vous permettent de gérer l'accès des utilisateurs et des ordinateurs aux ressources partagées et de filtrer les paramètres de règle de groupe.
- 1 **Distribution**-les groupes de distribution servent exclusivement de listes de distribution par courrier électronique.

Assurez-vous que le type de groupe demeure **Sécurité**. Vous ne pouvez pas utiliser les groupes de distribution pour attribuer des autorisations à des objets, ni les utiliser à des fins de filtrage des paramètres de règle de groupe.

Mon ouverture de session via Active Directory a échoué. Que dois-je faire ?

iDRAC6 intègre un outil de diagnostic dans l'interface Web.

1. Ouvrez une session en tant qu'utilisateur local avec droits d'administrateur depuis l'interface Web.
2. Dans l'arborescence du système, sélectionnez **Système**→ **Accès à distance**→ iDRAC6→ Onglet **Réseau/Sécurité**→ **Service d'annuaire**→ **Microsoft Active Directory**.

L'écran de résumé **Active Directory** apparaît.

3. Faites défiler jusqu'au bas de l'écran, puis cliquez sur **Paramètres du test**.

L'écran **Paramètres du test Active Directory** apparaît.

4. Entrez un nom d'utilisateur et 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. iDRAC6 enregistre également les résultats détaillés du test pour vous aider à résoudre tous les problèmes.

Si les problèmes persistent, configurez vos paramètres Active Directory, modifiez votre configuration utilisateur et exécutez à nouveau le test jusqu'à ce que l'utilisateur du test franchisse l'étape d'autorisation.

J'ai activé la validation du certificat, mais je ne suis pas parvenu à ouvrir une session sur Active Directory. J'ai exécuté les diagnostics depuis l'interface utilisateur et les résultats du test affichent le message d'erreur suivant. Quel peut être le problème et comment le résoudre ?

```
ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate. (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 d'annuaire).
```

Si la validation de certificat est activée, iDRAC6 utilise le certificat d'AC téléversé pour vérifier le certificat du serveur d'annuaire lorsqu'iDRAC6 établit la

connexion SSL avec le serveur d'annuaire. Les raisons les plus courantes de l'échec de la validation de certificat sont :

- 1 La date de l'iDRAC6 n'est pas comprise dans la période de validité du certificat de serveur ou du certificat d'autorité de certification. Vérifiez l'heure iDRAC6 et la période de validité de votre certificat.
- 1 Les adresses du contrôleur de domaine configurées dans l'iDRAC6 ne correspondent pas au sujet ou au nom alternatif du sujet du certificat de serveur d'annuaire.
 - o Si vous utilisez une adresse IP, consultez J'utilise une adresse IP pour une adresse de contrôleur de domaine, et je ne suis pas parvenu à valider le certificat. Quel est le problème ?.
 - o Si vous utilisez le nom de domaine complet, assurez-vous d'utiliser le nom de domaine complet du contrôleur de domaine, et non le domaine proprement dit. Par exemple, utilisez `servername.example.com`, et *non* `example.com`.

Que dois-je vérifier si je ne parviens pas à ouvrir une session iDRAC6 via Active Directory ?

Tout d'abord, diagnostiquez le problème à l'aide de la fonctionnalité Paramètres du test. Pour obtenir des instructions, consultez [Mon ouverture de session via Active Directory a échoué. Que dois-je faire ?](#).

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. Vous devez cependant généralement vérifier les éléments suivants :

1. Assurez-vous que vous utilisez le nom de domaine utilisateur correct pendant l'ouverture de session, et non le nom NetBIOS.
2. Si vous avez un compte utilisateur iDRAC6 local, ouvrez une session iDRAC6 à l'aide de vos références locales.
 - a. Assurez-vous que la case **Active Directory activé** est cochée dans la page **Étape 2 sur 4 Configuration et gestion d'Active Directory**.
 - b. Si vous avez activé la validation des certificats, assurez-vous que vous avez téléversé le certificat d'autorité de certification racine Active Directory correct sur iDRAC6. Le certificat apparaît dans la zone **Certificat d'autorité de certification d'Active Directory actuel**. Assurez-vous que l'heure de l'iDRAC6 est comprise dans la période de validité du certificat d'autorité de certification.
 - c. Si vous utilisez le schéma étendu, assurez-vous que le **Nom iDRAC6** et le **Nom de domaine iDRAC6** correspondent à la configuration de votre environnement Active Directory.

Si vous utilisez le schéma standard, assurez-vous que le **Nom du groupe** et le **Domaine du groupe** correspondent à votre configuration Active Directory.
 - d. Naviguez jusqu'à l'écran **Réseau**. Sélectionnez **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Réseau**. Assurez-vous que les paramètres du DNS sont corrects.
 - e. Vérifiez les certificats SSL du contrôleur de domaine pour vous assurer que l'heure iDRAC6 est comprise dans la période de validité du certificat.

Validation des certificats Active Directory

J'utilise une adresse IP pour une 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 corriger le problème en effectuant l'une des actions suivantes :

- 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.
- 1 Publier à nouveau le certificat de serveur de telle sorte à 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.
- 1 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.

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.

Schémas étendu et standard

J'utilise un schéma étendu dans un environnement à domaines multiples. Comment puis-je configurer les adresses du contrôleur de domaine ?

Utilisez le nom d'hôte (FQDN) ou l'adresse IP du ou des contrôleurs de domaine servant le domaine dans lequel l'objet iDRAC6 réside.

Dois-je configurer les adresses du catalogue global ?

Si vous utilisez le schéma étendu, il est impossible de configurer les adresses de catalogue global, car elles ne sont pas utilisées avec le schéma étendu.

Si vous utilisez le schéma standard, et que les utilisateurs et groupes de rôles proviennent de domaines différents, vous devez configurer les adresses du catalogue global. Dans ce cas, vous pouvez uniquement utiliser le groupe universel.

Si vous utilisez le schéma standard, et que les utilisateurs et groupes de rôles proviennent du même domaine, il n'est pas nécessaire de configurer les adresses du catalogue global.

Comment fonctionne la requête de schéma standard ?

iDRAC6 se connecte d'abord aux adresses de contrôleur de domaine configurées. Si l'utilisateur et les groupes de rôles résident dans ce domaine, les privilèges sont sauvegardés.

Si une ou des adresses de contrôleur globales sont configurées, iDRAC6 continue d'interroger le catalogue global. Si des privilèges supplémentaires sont récupérés du catalogue global, ces privilèges sont accumulés.

Divers

iDRAC6 utilise-t-il toujours LDAP sur SSL ?

Oui. Tous les transports se font via le port sécurisé 636 et/ou 3269.

Durant la *configuration du test*, l'iDRAC6 établit une connexion LDAP CONNECT uniquement pour aider à isoler le problème, mais n'effectue pas de LDAP BIND sur une connexion non sécurisée.

iDRAC6 prend-il en charge le nom NetBIOS ?

Pas dans cette version.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration d'iDRAC6 pour la connexion directe et l'ouverture de session par carte à puce

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [À propos de l'authentification Kerberos](#)
- [Configuration de l'ouverture de session par carte à puce sur iDRAC6](#)
- [Spécifications pour l'authentification par SSO et par carte à puce d'Active Directory](#)
- [Ouverture de session iDRAC6 via l'authentification par carte à puce Active Directory](#)
- [Utilisation de la fonctionnalité SSO Active Directory](#)
- [Questions les plus fréquentes sur SSO](#)
- [Configuration de l'authentification par carte à puce dans iDRAC6](#)
- [Dépannage de l'ouverture de session par carte à puce dans iDRAC6](#)

Cette section fournit des informations de configuration d'iDRAC6 pour l'ouverture de session par carte à puce pour les utilisateurs locaux et les utilisateurs d'Active Directory, et pour l'ouverture de session par connexion directe (SSO) pour les utilisateurs d'Active Directory.

iDRAC6 prend en charge l'authentification Active Directory Kerberos afin de prendre en charge les ouvertures de session par carte à puce et par connexion directe (SSO) Active Directory.

À propos de l'authentification Kerberos

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 maintenir aux normes de mise en application d'authentification renforcées, iDRAC6 prend désormais en charge l'authentification Active Directory Kerberos afin de pouvoir prendre en charge les ouvertures de session par carte à puce et par connexion directe (SSO) 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 mécanismes 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 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.

L'authentification Kerberos sur l'iDRAC6 échoue si l'heure de l'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** l'iDRAC6.

Vous pouvez également utiliser la commande de décalage du fuseau horaire RACADM suivante pour synchroniser l'heure :

```
racadm config -g cfgRacTuning -o
```

```
cfgRacTuneTimeZoneOffset <offset value>
```

Spécifications pour l'authentification par SSO et par carte à puce d'Active Directory

Les spécifications pour l'authentification par SSO et par carte à puce d'Active Directory sont les suivantes :

- 1 Configurez l'iDRAC6 en vue de l'ouverture de session Active Directory. Pour plus d'informations, consultez [Utilisation du service d'annuaire iDRAC6, page 141](#).
- 1 Enregistrez l'iDRAC6 comme un ordinateur dans le domaine racine Active Directory.
 - a. Cliquez sur **Système→Accès à distance→ iDRAC6→ Réseau/Sécurité→**, puis sur le sous-onglet **Réseau**.
 - b. Fournissez une adresse IP valide pour le **serveur DNS préféré/auxiliaire**. Cette valeur est l'adresse IP du DNS faisant partie du domaine racine et authentifiant les comptes Active Directory des utilisateurs.
 - c. Sélectionnez **Inscrire iDRAC6 sur DNS**.
 - d. Spécifiez un **nom de domaine DNS** valide.
 - e. Vérifiez que la configuration DNS du réseau correspond aux informations DNS d'Active Directory.

Consultez l'aide en ligne d'iDRAC6 pour plus d'informations.

- 1 Pour prendre en charge les deux nouveaux types de mécanisme d'authentification, iDRAC6 endosse 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 établir une correspondance entre iDRAC6 et un compte d'utilisateur dans Active Directory.

Par exemple, utilisez la commande **ktpass** suivante pour créer le fichier keytab Kerberos :

```
C:\> ktpass.exe -princ HTTP/idracname.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass <mot de passe> +DesOnly -out c:\krbkeytab
```

 **REMARQUE** : En cas de problèmes avec l'utilisateur iDRAC6 pour lequel le fichier keytab est créé, créez un nouvel utilisateur et un nouveau fichier keytab. Si le fichier keytab initialement créé est exécuté à nouveau, il ne configurera pas correctement.

Une fois l'exécution des commandes ci-dessus réussie, exécutez la commande suivante :

```
C:\>setspn -a HTTP/idracname.domainname.com username
```

Le type de cryptage qu'iDRAC6 utilise pour l'authentification Kerberos est DES-CBC-MD5. Le type principal est KRB5_NT_PRINCIPAL. La propriété Utiliser les types de cryptage DES pour ce compte doit être activée dans les propriétés du compte d'utilisateur auquel est associé le nom principal du service.

 **REMARQUE** : Vous devez créer un compte utilisateur Active Directory qui sera utilisé avec l'option **-mapuser** de la commande **ktpass**. Vous devez également avoir le même nom que le nom DNS iDRAC6 vers lequel vous téléverserez le fichier keytab généré.

 **REMARQUE** : Il est recommandé d'utiliser le dernier utilitaire **ktpass** pour créer le fichier keytab. En outre, pendant la génération du fichier keytab, utilisez des lettres *minuscules* pour le **nom de l'iDRAC** et le **nom principal du service**.

Cette procédure génère un fichier keytab que vous devrez téléverser dans l'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**, accédez au site Web de Microsoft à l'adresse : [http://technet.microsoft.com/en-us/library/cc779157\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx)

- 1 L'heure d'iDRAC6 doit être synchronisée avec celle du contrôleur de domaine Active Directory.

Paramètres du navigateur afin d'activer la fonctionnalité SSO Active Directory

Pour configurer les paramètres du navigateur pour Internet Explorer :

1. Ouvrez le navigateur Web Internet Explorer.
2. Sélectionnez **Outils** → **Options Internet** → **Sécurité** → **Intranet local**.
3. Cliquez sur **Sites**.
4. Sélectionnez les options suivantes uniquement :
 - 1 Inclure tous les sites locaux (intranet) non mentionnés dans d'autres zones.
 - 1 Inclure tous les sites qui n'utilisent pas de serveur proxy.
5. Cliquez sur **Avancé**.
6. Ajoutez tous les noms de domaine relatifs qui seront utilisés pour les instances iDRAC faisant partie de la configuration SSO (par exemple, myhost.example.com.)
7. Cliquez sur **Fermer**, puis sur **OK**.
8. Cliquez sur **OK**.

Pour configurer les paramètres du navigateur pour Firefox :

1. Ouvrez le navigateur Web Firefox.
 2. Dans la barre d'adresses, entrez `about:config`.
 3. Dans **Filtre**, entrez `network.negotiate`.
 4. Ajoutez le nom iDRAC à `network.negotiate-auth.trusted-uris` (en utilisant une liste avec séparation par des virgules).
 5. Ajoutez le nom iDRAC à `network.negotiate-auth.delegation-uris` (en utilisant une liste avec séparation par des virgules).
-

Utilisation de la fonctionnalité SSO Active Directory

Vous pouvez activer l'iDRAC6 pour utiliser Kerberos, un protocole d'authentification réseau, afin de permettre la connexion directe. Pour plus d'informations sur la configuration d'iDRAC6 pour utiliser la fonctionnalité de connexion directe d'Active Directory, consultez [Spécifications pour l'authentification par SSO et par carte à puce d'Active Directory](#).

Configuration d'iDRAC6 pour utiliser la fonctionnalité SSO

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** → **Accès à distance** → iDRAC6 → **Onglet Réseau/Sécurité** → **Réseau**. Sur la page **Réseau**, vérifiez que le **Nom iDRAC6 DNS** est correct et correspond au nom utilisé pour le nom de domaine pleinement qualifié de l'iDRAC6.
4. Dans l'arborescence du système, sélectionnez **Système** → **Accès à distance** → iDRAC6 → Onglet **Réseau/Sécurité** → **Service d'annuaire** → **Microsoft Active Directory**.
L'écran de résumé Active Directory apparaît.

5. Faites défiler jusqu'au bas de l'écran, puis cliquez sur **Configurer Active Directory**.

L'écran **Configuration et gestion d'Active Directory Étape 1 sur 4** s'affiche.

6. Pour valider le certificat SSL des serveurs Active Directory, cochez la case **Activer la validation des certificats** sous **Paramètres des certificats**.

Si vous ne voulez pas valider le certificat SSL de vos serveurs Active Directory, n'effectuez aucune action et passez à [étape 8](#).

7. Sous **Téléverser le certificat d'autorité de certification d'Active Directory**, entrez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat, puis cliquez sur **Téléverser**.

 **REMARQUE :** Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

Les informations relatives au certificat d'autorité de certification d'Active Directory que vous avez téléversé s'affichent dans la section **Certificat d'autorité de certification d'Active Directory actuel**.

8. Cliquez sur **Suivant**.

L'écran **Configuration et gestion d'Active Directory Étape 2 sur 4** s'affiche.

9. Cochez la case **Activer Active Directory**.

10. Sélectionnez **Activer la connexion directe** si vous souhaitez ouvrir une session iDRAC6 directement après vous êtes connecté à votre station de travail sans entrer vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe.

Pour ouvrir une session iDRAC6 à l'aide de cette fonctionnalité, vous devez impérativement être déjà connecté à votre système via un compte utilisateur Active Directory valide. En outre, vous devez déjà avoir configuré le compte utilisateur pour ouvrir une session iDRAC6 à l'aide des références d'Active Directory. iDRAC6 utilise les références d'Active Directory mises en cache pour vous connecter.

Avant de configurer iDRAC6 pour utiliser la connexion directe (SSO), vérifiez que vous avez bien effectué les opérations ci-dessous :

- a. Création de l'objet Périphérique, de l'objet Privilège et de l'objet Association sur le serveur Active Directory.
- b. Définition des privilèges d'accès à l'objet Privilège créé. Il est recommandé de ne pas fournir de privilèges Administrateur qui risqueraient d'ignorer certains contrôles de sécurité.
- c. Association de l'objet Périphérique et de l'objet Privilège au moyen de l'objet Association.
- d. Ajout de l'utilisateur SSO précédent (utilisateur d'ouverture de session) à l'objet Périphérique.
- e. Octroi d'un privilège d'accès aux *Utilisateurs authentifiés* afin de leur permettre d'accéder à l'objet Association créé.

Pour des informations sur la réalisation de ces étapes, consultez [Ajout d'utilisateurs iDRAC6 et de leurs privilèges à Active Directory](#), page 160.

Pour activer SSO à l'aide de la CLI, exécutez la commande RACADM :

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

11. Ajoutez le **Nom de domaine de l'utilisateur**, puis entrez l'adresse IP du serveur du contrôleur de domaine. Sélectionnez **Rechercher les contrôleurs de domaine avec DNS** ou **Définir des adresses de contrôleur de domaine**. Cliquez sur **Suivant**. L'écran **Configuration et gestion d'Active Directory Étape 3 sur 4** s'affiche.

12. Sélectionnez l'option **Schéma standard** ou **Schéma étendu** et cliquez sur **Suivant**.

Si vous avez sélectionné **Schéma standard**, passez à l'étape 13. Si vous avez sélectionné **Schéma étendu**, passez à l'étape 14.

13. Pour le schéma standard :
 - a. Dans l'écran **Active Directory Étape 4a sur 4**, entrez l'adresse IP du **Serveur de catalogue global** ou sélectionnez l'option **Rechercher des serveurs de catalogue global avec DNS** et entrez le **Nom de domaine racine** à utiliser pour une recherche DNS afin d'obtenir les serveurs de catalogue global Active Directory.
 - b. Cliquez sur l'un des groupes de rôles et ajoutez les informations du groupe de rôles dont votre utilisateur Active Directory valide est membre. L'écran **Active Directory Étape 4b sur 4** apparaît.
 - c. Entrez le nom du groupe de rôles, le domaine du groupe, le niveau de privilèges du groupe de rôles et les privilèges requis, puis cliquez sur **Terminer**. Le message "Configuration set successfully" (« Configuration définie correctement ») apparaît.. Cliquez sur **OK**. L'écran **Étape 4a sur 4** affiche le nom du groupe de rôles créé, le domaine du groupe et le niveau de privilèges du groupe.
 - d. Cliquez sur **Terminer**. Le message de réussite s'affiche.
14. Pour le schéma étendu, dans l'écran **Active Directory Étape 4 sur 4**, entrez le **Nom iDRAC6** et le **Nom de domaine iDRAC6**, puis cliquez sur **Terminer**. Le message de réussite s'affiche.

Ouverture de session iDRAC6 via SSO

1. Connectez-vous à votre station de gestion avec votre compte réseau Active Directory valide.
2. Connectez-vous à la page Web iDRAC6 avec le nom de domaine pleinement qualifié d'iDRAC6 :

`http://idracname.domain.com`.

L'iDRAC6 vous connecte à l'aide de vos références mises en cache dans le système d'exploitation lorsque vous vous connectez via votre compte réseau Active Directory valide.

Configuration de l'authentification par carte à puce

L'iDRAC6 prend en charge la fonctionnalité d'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 fonctionnalité 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 NIP).

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 d'ouverture de session par carte à puce iDRAC6 à partir de l'interface Web :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Accédez à l'écran **Étape 1 sur 4 Configuration et gestion d'Active Directory**.
4. Pour valider le certificat SSL de vos serveurs Active Directory, cochez la case **Validation des certificats activée** sous **Paramètres des certificats**. Si vous ne souhaitez pas valider le certificat SSL de vos serveurs Active Directory, passez à [étape 6](#).
5. Sous **Téléverser le certificat d'autorité de certification d'Active Directory**, entrez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat, puis cliquez sur **Téléverser**. Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier. Les informations relatives au certificat d'autorité de certification d'Active Directory que vous avez téléversé s'affichent dans la section **Certificat d'autorité de certification d'Active Directory actuel**.
6. Cliquez sur **Suivant**. L'écran **Étape 2 sur 4 Configuration et gestion d'Active Directory** apparaît.
7. Cochez la case **Active Directory activé**.
8. Sélectionnez **Activer l'ouverture de session par carte à puce** afin d'activer l'ouverture de session par carte à puce. Vous serez invité à ouvrir une session par carte à puce lors de chaque tentative ultérieure d'ouverture de session via l'interface utilisateur graphique.
9. Ajoutez le **Nom de domaine de l'utilisateur**, puis entrez l'adresse IP du serveur du contrôleur de domaine. Cliquez sur **Suivant**.
10. Sélectionnez **Paramètres du schéma standard** sur la page **Étape 3 sur 4 Configuration et gestion d'Active Directory**. Cliquez sur **Suivant**.
11. Sur la page **Étape 4a sur 4 Active Directory**, entrez l'adresse IP du **serveur de catalogue global**. Ajoutez les informations du groupe de rôles dont

votre utilisateur Active Directory valide est membre, en sélectionnant un des groupes de rôles (page **Étape 4B sur 4 Configurer le groupe de rôles**). Entrez le **Nom du groupe**, le **Domaine du groupe** et les **Privilèges de groupe de rôles**. Cliquez sur **OK**, puis sur **Terminer**. Après avoir sélectionné **Terminé**, revenez au bas de la page de résumé Active Directory, puis sélectionnez **Téléversement du fichier keytab Kerberos**.

12. Téléversez un fichier keytab Kerberos valide. Assurez-vous que l'heure du serveur Active Directory et celle de l'iDRAC6 sont synchronisées. Vérifiez que les heures et les fuseaux horaires sont corrects avant de téléverser le fichier keytab. Pour plus d'informations sur la création d'un fichier keytab, consultez [Configuration d'iDRAC6 pour la connexion directe et l'ouverture de session par carte à puce](#).

Décochez la case **Activer l'ouverture de session par carte à puce** pour désactiver la fonctionnalité TFA Ouverture de session par carte à puce. À la prochaine ouverture de session sur l'interface utilisateur d'iDRAC6, vous serez 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 depuis l'interface Web.

Ouverture de session iDRAC6 via l'authentification par carte à puce Active Directory

 **REMARQUE :** Selon les paramètres de votre navigateur, il se peut que vous soyez invité à télécharger et installer le plug-in ActiveX du lecteur de carte à puce lorsque vous utilisez cette fonctionnalité pour la première fois.

1. Ouvrez une session 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 de l'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.
3. Saisissez le code NIP, puis cliquez sur **Ouverture de session**.

Vous avez ouvert une session iDRAC6 avec vos références telles qu'elles sont configurées dans Active Directory.

 **REMARQUE :** Il n'est pas nécessaire de laisser votre carte à puce dans le lecteur pour que votre session reste ouverte.

Questions les plus fréquentes sur SSO

L'ouverture de session par SSO échoue sous Windows 7 et Windows Server 2008 R2.

Vous devez activer les types de cryptage DES_CBC_CRC et DES_CBC_MD5 pour Windows 7 et Windows Server 2008 R2. Pour activer les types de cryptage :

1. Ouvrez une session en tant qu'administrateur ou en tant qu'utilisateur doté des privilèges Administrateur.
2. Accédez à **Démarrer** et exécutez `gpedit`. La fenêtre **Éditeur de règles de groupe local** s'affiche.
3. Accédez à **Paramètres de l'ordinateur local** → **Paramètres Windows** → **Paramètres de sécurité** → **Règles locales** → **Options de sécurité**.
4. Cliquez-droite sur **Sécurité réseau : Configurer les types de cryptage autorisés pour Kerberos** et sélectionnez **Propriétés**.
5. Activez toutes les options.
6. Cliquez sur **OK**.

Dépannage de l'ouverture de session par carte à puce dans iDRAC6

Utilisez les astuces suivantes pour déboguer une carte à puce inaccessible :

L'ouverture d'une session iDRAC6 avec l'ouverture de session par carte à puce Active Directory prend presque 4 minutes.

L'ouverture de session normale par carte à puce Active Directory nécessite généralement moins de 10 secondes, mais l'ouverture de session sur iDRAC6 à l'aide de l'ouverture de session par carte à puce Active Directory peut prendre presque 4 minutes si vous avez spécifié **Serveur DNS préféré** et **Serveur DNS auxiliaire** dans la page **Réseau** iDRAC6 et qu'une panne du serveur DNS préféré est survenue. Des expirations du délai d'attente DNS peuvent se produire

lorsque le serveur DNS est en panne. iDRAC6 vous connecte à l'aide du serveur DNS auxiliaire.

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 NIP 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 iDRAC6 en tant qu'utilisateur Active Directory

- 1 Si vous ne parvenez pas à ouvrir une session iDRAC6 en tant qu'utilisateur Active Directory, essayez d'ouvrir une session iDRAC6 sans activer l'ouverture de session par carte à puce. Vous pouvez désactiver l'ouverture de session par carte à puce via la RACADM en utilisant la commande suivante :

```
racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0
```

- 1 Pour les plateformes Windows 64 bits, le plug-in d'authentification d'iDRAC6 ne s'installe pas correctement si une version 64 bits du progiciel redistribuable Microsoft Visual C++ 2005 est déployée. Pour que le plug-in s'installe et s'exécute correctement, vous devez déployer la version 32 bits du progiciel redistribuable Microsoft Visual C++ 2005.
- 1 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, mais 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. 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 toutes deux le chargement du plug-in de carte à puce Dell :

Tableau 7-1. 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

- 1 Vérifiez que la différence entre l'heure de l'iDRAC6, l'heure du contrôleur de domaine et celle du serveur du contrôleur de domaine est de 5 minutes au plus, afin que l'authentification Kerberos puisse fonctionner. Vérifiez l'heure iDRAC6 sur la page **Système** → **Accès à distance** → **iDRAC6** → **Propriétés** → **Informations sur l'accès à distance** et l'heure du contrôleur de domaine en cliquant avec le bouton droit de la souris sur l'heure en bas à droite 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 iDRAC6 (via la RACADM distante ou Telnet/SSH) : `racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <valeur du décalage en minutes>`. Par exemple, si l'heure du 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](#)

Visualisation de la configuration et de l'intégrité du serveur géré

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Résumé du système](#)
- [Détails du système](#)
- [WWN/MAC](#)
- [Intégrité du serveur](#)

Résumé du 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**, cliquez sur **Système** → onglet **Propriétés** → **Résumé du système**. Consultez l'aide en ligne d'iDRAC6 pour des informations détaillées sur chaque section de la page **Résumé du système**.

Détails du système

La page **Détails du système** affiche des informations sur les composants système suivants :

- 1 Enceinte principale du système
- 1 Integrated Dell Remote Access Controller 6 - Enterprise

Enceinte principale du système

Informations système

Cette section de l'interface Web iDRAC6 fournit les informations de base suivantes sur le serveur géré :

- 1 Description - le numéro de modèle ou le nom du serveur géré
- 1 Version du BIOS - le numéro de version du BIOS du serveur géré
- 1 Numéro de service - le numéro de service du serveur
- 1 Nom d'hôte - le nom d'hôte DNS associé au serveur géré
- 1 Nom du système d'exploitation - le nom du système d'exploitation installé sur le serveur géré

 **REMARQUE** : Le champ **Nom du système d'exploitation** est renseigné uniquement si Dell OpenManage Server Administrator est installé sur le système géré. Les noms des systèmes d'exploitation VMware constituent une exception : ils sont affichés, même si Server Administrator n'est pas installé sur le système géré.

- 1 Révision du système - numéro de révision du châssis.

Carte mezzanine d'E/S

Cette section de l'interface Web iDRAC6 fournit les informations suivantes sur les cartes mezzanines d'E/S installées sur le serveur géré :

- 1 Emplacement - énumère la ou les cartes mezzanines d'E/S installées sur le serveur géré. La liste affiche également les cartes mezzanines d'E/S pour les plateformes prenant en charge les cartes d'extension.
- 1 Condition de présence - indique si la carte mezzanine est présente ou non ou s'il s'agit d'une extension du logement de la carte mezzanine d'une autre structure.
- 1 Type de carte - le type physique de la carte mezzanine installée/de la connexion.
- 1 Nom du modèle - le numéro du modèle, le type ou la description de la ou des cartes mezzanines installées.

Carte de stockage intégrée

Cette section de l'interface Web iDRAC6 fournit des informations sur la carte du contrôleur de stockage intégrée installée sur le serveur géré :

- 1 Type de carte - affiche le nom du modèle de la carte de stockage installée, par exemple SAS6/iR

Carte réseau intégrée

Cette section de l'interface Web iDRAC6 fournit des informations sur la carte réseau intégrée installée sur le serveur géré. Elle apparaît uniquement pour les plateformes concernées.

- 1 Type de carte - affiche le type de carte de la carte réseau intégrée installée sur la carte, par exemple Gigabit Ethernet.
- 1 Nom du modèle - affiche le nom du modèle de la carte réseau intégrée.

Pour plus d'informations sur la carte réseau intégrée, consultez le *Manuel du propriétaire du matériel* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Récupération automatique

Cette section de l'interface Web iDRAC6 détaille le mode actuel de fonctionnement de la fonctionnalité Récupération automatique du serveur géré comme définie par Open Manage Server Administrator :

- 1 Action de récupération - action à effectuer en cas de détection d'une défaillance ou d'une *suspension* du système. Les actions disponibles sont **Pas d'action**, **Réinitialisation matérielle**, **Mise hors tension** ou **Cycle d'alimentation**.
- 1 Compte à rebours initial - le laps de temps (en secondes) après lequel une suspension du système est détectée et où iDRAC6 effectue une action de récupération.
- 1 Compte à rebours présent - la valeur actuelle (en secondes) du temporisateur de compte à rebours.

Integrated Dell Remote Access Controller 6 - Enterprise

Informations sur iDRAC6

Cette section de l'interface Web iDRAC6 fournit les informations suivantes sur iDRAC6 lui-même :

- 1 Date/Heure - affiche les date et heure actuelles (à compter de la dernière actualisation de la page) de l'iDRAC6
- 1 Version du micrologiciel - affiche la version actuelle du micrologiciel iDRAC6 installé sur le système géré
- 1 Version du CPLD - affiche la version du périphérique logique programmable complexe (CPLD) de la carte.
- 1 Version du CPLD étendu - affiche la version du CPLD étendu de la carte.
- 1 Micrologiciel mis à jour - affiche les date et heure de la dernière mise à jour réussie du micrologiciel iDRAC6
- 1 Adresse MAC - affiche l'adresse MAC associée au contrôleur d'interface réseau LOM (LAN sur carte mère) de l'iDRAC6

Paramètres IPv4

- 1 Activé - affiche si la prise en charge du protocole IPv4 est activée ou désactivée.
 -  **REMARQUE** : L'option Protocole IPv4 est activée par défaut.
- 1 DHCP activé - activé si iDRAC6 est défini pour chercher son adresse IP et les infos associées auprès d'un serveur DHCP
- 1 Adresse IP - affiche l'adresse IP associée à iDRAC6 (et non au serveur géré)
- 1 Masque de sous-réseau - affiche le masque de sous-réseau TCP/IP configuré pour iDRAC6
- 1 Passerelle - affiche l'adresse IP de la passerelle réseau configurée pour iDRAC6
- 1 Utiliser DHCP pour obtenir des adresses de serveur DNS - affiche si DHCP est utilisé pour obtenir des adresses de serveur DNS
- 1 Serveur DNS préféré - affiche le serveur DNS principal actuellement actif
- 1 Serveur DNS auxiliaire - affiche l'adresse d'un serveur DNS auxiliaire

Paramètres IPv6

- 1 Activé - affiche si la prise en charge du protocole IPv6 est activée ou désactivée
- 1 Configuration automatique activée - affiche si la configuration automatique est activée ou désactivée
- 1 Adresse locale de lien - affiche l'adresse IPv6 du NIC d'iDRAC6
- 1 Adresse IPv6 1-16 - affiche jusqu'à 16 adresses IPv6 (adresse IPv6 1 à adresse IPv6 16) pour le NIC d'iDRAC6.
- 1 Passerelle - affiche l'adresse IP de la passerelle réseau configurée pour iDRAC6
- 1 Utiliser DHCPv6 pour obtenir des adresses de serveur DNS - affiche si DHCP est utilisé pour obtenir des adresses de serveur DNS
- 1 Serveur DNS préféré - affiche le serveur DNS principal actuellement actif

- 1 Serveur DNS auxiliaire - affiche l'adresse d'un serveur DNS auxiliaire

 **REMARQUE :** Ces informations sont également disponibles dans iDRAC6 → **Propriétés** → **Informations sur l'accès à distance**.

Adresses MAC du NIC intégré

- 1 NIC 1 - affiche les adresses de contrôle de l'accès aux médias (MAC) 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.

- 1 NIC 2 - affiche les adresses MAC du contrôleur d'interface réseau 2 intégré qui l'identifie de façon unique sur le réseau.
- 1 NIC 3 - affiche les adresses MAC du contrôleur d'interface réseau 3 intégré qui l'identifie de façon unique sur le réseau. Les adresses MAC du contrôleur d'interface réseau 3 intégré peuvent ne pas s'afficher sur tous les systèmes.
- 1 NIC 4 - affiche les adresses MAC du contrôleur d'interface réseau 4 intégré qui l'identifie de façon unique sur le réseau. Les adresses MAC du contrôleur d'interface réseau 4 intégré peuvent ne pas s'afficher sur tous les systèmes.

WWN/MAC

Cliquez sur **Système** → onglet **Propriétés** → **WWN/MAC** pour visualiser la configuration actuelle des cartes mezzanines d'E/S installées et la structure des réseaux associés. Si la fonctionnalité FlexAddress est activée dans CMC, les adresses MAC persistantes assignées globalement (assignées au châssis) remplacent les valeurs câblées de chaque LOM.

Intégrité du serveur

Cliquez sur **Système** → onglet **Propriétés** → **Résumé du système** → **Intégrité du serveur** pour afficher des informations importantes sur l'intégrité d'iDRAC6 et des composants surveillés par iDRAC6. La colonne **Condition** indique la condition de chaque composant. Pour une liste des icônes de condition et leur signification, consultez [Tableau 19-3](#). Cliquez sur le nom du composant dans la colonne **Composant** pour plus d'informations détaillées sur le composant.

 **REMARQUE :** Pour obtenir les informations sur le composant, vous pouvez également cliquer sur le nom du composant dans le volet gauche de la fenêtre. Les composants restent visibles dans le volet gauche, indépendamment de l'onglet/l'écran sélectionné.

iDRAC6

L'écran **Informations sur l'accès à distance** répertorie plusieurs détails importants sur iDRAC6, tels que le nom, la révision du micrologiciel, le micrologiciel mis à jour, l'heure iDRAC6, la version d'IPMI, la version de CPLD, le type de serveur et les paramètres réseau. Pour obtenir des détails supplémentaires, cliquez sur l'onglet approprié en haut de l'écran.

CMC

L'écran CMC affiche la condition d'intégrité, la révision du micrologiciel et les adresses IP de Chassis Management Controller. Vous pouvez également lancer l'interface Web de CMC en cliquant sur le bouton **Lancer l'interface Web de CMC**. Consultez le [Guide d'utilisation du micrologiciel Chassis Management Controller](#) pour obtenir plus d'informations.

 **REMARQUE :** Le lancement de l'interface utilisateur Web de CMC à partir d'iDRAC6 dirige votre recherche avec le même format d'adresse IP. Par exemple, si vous ouvrez l'interface utilisateur Web iDRAC6 avec un format d'adresse IPv6, la page Web de CMC s'ouvrira également avec une adresse IPv6 valide.

Piles

L'écran **Piles** affiche la condition et les valeurs de la pile bouton de la carte système qui permet de stocker les données de configuration de l'horloge en temps réel (RTC) et CMOS du système géré.

Températures

L'écran **Températures** affiche la condition et les mesures du capteur de température ambiante intégré. Les seuils de température minimum et maximum correspondant à l'état *avertissement* et *défaillance* sont affichés avec la condition d'intégrité actuelle du capteur.

 **REMARQUE :** Selon le modèle de votre serveur, les seuils de température des états *avertissement* ou *défaillance* et/ou la condition d'intégrité du capteur peuvent ne pas s'afficher.

Tensions

L'écran **Capteurs de tension** affiche la condition et la mesure des capteurs de tension, donnant des informations telles que la condition des capteurs de noyau CPU et de pôle de tension intégrés.

Contrôle de l'alimentation

L'écran **Contrôle de l'alimentation** vous permet de visualiser les informations suivantes relatives au contrôle et aux statistiques d'alimentation :

- 1 Contrôle de l'alimentation - affiche la quantité d'alimentation consommée (valeur de puissance moyenne sur une minute mesurée en watts CA) par le serveur telle que communiquée par le moniteur de courant de la carte système.
- 1 Intensité - affiche la consommation actuelle (CA en ampères) dans l'unité d'alimentation active.
- 1 Statistiques de consommation de puissance - affiche des informations sur l'alimentation consommée par le système depuis la dernière réinitialisation de la mesure.
- 1 Statistiques de consommation maximale - affiche des informations sur l'alimentation maximale consommée par le système depuis la dernière réinitialisation de la mesure.
- 1 Consommation énergétique - affiche la consommation énergétique moyenne, minimale et maximale, et les heures de puissance maximale et minimale dans le système au cours de la minute, de l'heure, de la journée et de la semaine précédente.
- 1 Afficher graphique - affiche une représentation graphique de la consommation énergétique sur 1 heure, 24 heures, 3 jours et 1 semaine.

 **REMARQUE** : La puissance et l'intensité sont mesurées en CA.

UC

L'écran **UC** indique l'intégrité de chaque UC sur le serveur géré. Cette condition d'intégrité est un cumul de plusieurs tests thermiques, d'alimentation et fonctionnels individuels.

POST

L'écran **Code POST** affiche le dernier code POST du système (au format hexadécimal) avant l'amorçage du système d'exploitation du serveur géré.

Intégrité div

L'écran **Intégrité div** permet d'accéder aux journaux système suivants :

- 1 Journal des événements système (SEL) - affiche les événements critiques qui se produisent sur le système géré.
- 1 Code POST - affiche le dernier code POST du système (au format hexadécimal) avant l'amorçage du système d'exploitation du serveur géré.
- 1 Écran de la dernière panne - affiche l'écran et l'heure de la dernière panne.
- 1 Saisie de l'amorçage - permet de lire les trois derniers écrans d'amorçage.

 **REMARQUE** : Ces informations sont également disponibles dans **Système** → onglet **Journaux** → **Journal des événements système**.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Contrôle et gestion de l'alimentation

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Configuration et gestion de l'alimentation](#)
- [Contrôle de l'alimentation](#)
- [Allocation d'énergie](#)
- [Contrôle de l'alimentation](#)

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 contrôler et de gérer l'alimentation.

 **REMARQUE :** La logique de gestion de l'alimentation iDRAC6 fait appel à un périphérique logique programmable complexe (Complex Programmable Logic Device, CPLD) présent dans le serveur lame. Quelques plateformes prennent également en charge un CPLD étendu. Les mises à jour des périphériques CPLD sont disponibles sur le site Web du support de Dell à l'adresse support.dell.com dans les sections **Micrologiciel système** ou **Carte système**. Il est recommandé de mettre votre serveur lame à jour avec la dernière version du micrologiciel CPLD. Les versions de micrologiciel du CPLD actuel et du CPLD étendu (pour les plateformes concernées) sont affichées dans l'interface utilisateur Web d'iDRAC6.

Les systèmes Dell PowerEdge offrent de nombreuses fonctionnalités de contrôle et de gestion de l'alimentation :

- 1 **Contrôle de l'alimentation :** iDRAC6 collecte un historique des mesures de consommation et calcule les moyennes, les pics, etc. À l'aide de l'interface Web iDRAC6, vous pouvez afficher les informations dans l'écran **Contrôle de l'alimentation**. Vous pouvez également afficher les informations sous forme de graphique en cliquant sur **Afficher le graphique** au bas de l'écran **Contrôle de l'alimentation**. Consultez la section [Contrôle de l'alimentation](#) pour plus d'informations.
- 1 **Bilan de puissance :** au démarrage, un inventaire système permet de calculer un bilan de puissance du système de la configuration actuelle. Consultez la section [Allocation d'énergie](#) pour plus d'informations.
- 1 **Contrôle de l'alimentation :** iDRAC6 vous permet d'effectuer à distance plusieurs actions de gestion de l'alimentation sur le système géré. Consultez la section [Contrôle de l'alimentation](#) pour plus d'informations.

Configuration et gestion de l'alimentation

Vous pouvez utiliser l'interface Web iDRAC6 et l'interface de ligne de commande RACADM (CLI) pour gérer et configurer les commandes d'alimentation du système Dell PowerEdge. Vous pouvez notamment :

- 1 afficher l'état de l'alimentation du serveur ; Consultez [Affichage du contrôle de l'alimentation](#).
- 1 afficher les informations du bilan de puissance du serveur, y compris la consommation énergétique potentielle maximale et minimale ; Consultez [Affichage du bilan de puissance](#).
- 1 afficher le seuil du bilan de puissance du serveur ; Consultez [Seuil du bilan de puissance](#).
- 1 afficher la puissance allouée aux cartes d'extension PCIe dans le serveur ; Consultez [Affichage et modification de l'allocation de puissance PCIe](#).
- 1 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 et arrêt normal). Consultez [Exécution de tâches de contrôle de l'alimentation sur un serveur](#).

Contrôle de l'alimentation

iDRAC6 surveille continuellement la consommation énergétique des serveurs Dell PowerEdge. L'iDRAC6 calcule les valeurs de puissance suivantes et fournit les informations via son interface Web ou la CLI RACADM :

- 1 Puissance système cumulée
- 1 Puissance système maximale et intensité système maximale
- 1 Consommation énergétique moyenne, minimale et maximale
- 1 Consommation énergétique (également affichée sous forme de graphiques dans l'interface Web)
- 1 Heures de consommation max. et min

Affichage du contrôle de l'alimentation

Utilisation de l'interface Web

Pour afficher les données de contrôle de l'alimentation :

- 1 Ouvrez une session sur l'interface Web iDRAC6.
- 2 Dans l'arborescence du système, sélectionnez **Contrôle de l'alimentation**.

L'écran **Contrôle de l'alimentation** apparaît, affichant les informations suivantes :

Contrôle de l'alimentation

- 1 **État** : une case verte indique que l'état de l'alimentation est normal, **Avertissement** indique qu'une alerte d'avertissement a été émise et **Critique** indique qu'une alerte de panne a été générée.
- 1 **Nom de capteur** : répertorie le nom du capteur.
- 1 **Lecture** : indique la puissance relevée par le capteur.
- 1 **Seuil d'avertissement** : affiche la consommation énergétique acceptable (en watts et en BTU/h) recommandée pour le fonctionnement du système. Une consommation énergétique qui excéderait cette valeur entraînerait des événements d'avertissement.
- 1 **Seuil de panne** : affiche la consommation énergétique la plus élevée acceptable (en watts et en BTU/h) requise pour le fonctionnement du système. Une consommation énergétique qui excéderait cette valeur entraînerait des événements critiques/de panne.

Intensité du courant

- 1 **Emplacement** : affiche le nom du capteur de carte système.
- 1 **Lecture** : la consommation actuelle en ampères CA.

Statistiques de consommation de puissance et statistiques de consommation maximale

- 1 **Statistiques** :
 - o **Puissance système cumulée** affiche la consommation énergétique cumulée (en kWh) du serveur. La valeur représente l'énergie totale utilisée par le système. Vous pouvez réinitialiser cette valeur sur 0 en cliquant sur **Réinitialiser** à la fin de la ligne du tableau.
 - o **Puissance système maximale** spécifie la valeur système maximale en watts CA.
 - o **Intensité système maximale** spécifie l'intensité système maximale. La valeur maximale est la valeur la plus élevée enregistrée entre l'heure de début des mesures et le moment actuel. L'heure de consommation maximale est celle où la valeur maximale a été atteinte. Cliquez sur **Réinitialiser** à la fin de la ligne du tableau pour rétablir la valeur instantanée actuelle (qui, si le serveur fonctionne, ne sera pas 0). Cliquez sur **Réinitialiser** rétablira également l'heure de début des mesures sur l'heure actuelle.
 - o **Heure de début des mesures** affiche la date et l'heure enregistrées depuis que la dernière valeur relative à la consommation énergétique du système a été effacée et qu'un nouveau cycle de mesures a débuté. Pour les statistiques de **Puissance système cumulée**, d'**Intensité système maximale** et de **Puissance système maximale**, la réinitialisation des valeurs de puissance maximale les ramène immédiatement à la valeur instantanée actuelle.
 - o **Heure actuelle de la mesure pour Puissance système cumulée** affiche la date et l'heure de calcul de la consommation énergétique du système pour l'affichage. Pour **Intensité système maximale** et **Puissance système maximale**, les champs **Heure de consommation maximale** affichent l'heure à laquelle ces pics se sont produits.
 - o **Lecture** : la valeur de la statistique appropriée - **Puissance système cumulée**, **Puissance système maximale** et **Intensité système maximale** depuis le démarrage du compteur.

 **REMARQUE** : Les statistiques de consommation de puissance sont conservées lors des réinitialisations du système, reflétant ainsi l'ensemble des activités qui se sont produites dans l'intervalle entre les heures de début et les heures actuelles indiquées. Les valeurs de puissance affichées dans le tableau de consommation de puissance sont des moyennes cumulatives au cours de l'intervalle de temps respectif (dernière minute, dernière heure, dernier jour et dernière semaine). 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 énergétique

- 1 **Consommation de puissance moyenne** : moyenne de la minute précédente, heure précédente, jour précédent et semaine précédente.
- 1 **Consommation de puissance maximale** et **Consommation de puissance minimale** : les consommations de puissance maximales et minimales observées au cours de l'intervalle de temps donné.
- 1 **Heure de puissance max** et **Heure de puissance min** : les heures (minute, heure, jour et semaine) auxquelles les consommations de puissance maximales et minimales se sont produites.

Afficher le graphique

Cliquez sur **Afficher graphique** pour afficher des graphiques illustrant la consommation énergétique en watts d'iDRAC6 au cours de la dernière heure, des dernières 24 heures, des trois derniers jours et de la semaine dernière. Utilisez le menu déroulant fourni au-dessus du graphique pour sélectionner la période.

 **REMARQUE** : Chaque point de données tracé sur les graphiques représente la moyenne des lectures sur une période de 5 minutes. Par conséquent, les graphiques peuvent ne pas refléter les brèves fluctuations d'alimentation électrique ou de courant.

Allocation d'énergie

L'écran **Bilan de puissance** affiche ces limites de seuil d'alimentation, qui couvrent la gamme des consommations en courant alternatif qu'un système soumis à une lourde charge de travail présentera au centre de données.

Avant la mise sous tension d'un serveur, iDRAC6 fournit à CMC les exigences de son enveloppe de puissance. Une fois le serveur sous tension, une enveloppe de puissance plus petite peut être requise, en fonction de la consommation de puissance réelle du serveur. Si la consommation de puissance augmente au fil du temps et que la consommation de puissance du serveur atteint son allocation maximale, iDRAC6 peut demander une hausse de la consommation énergétique potentielle maximale, augmentant ainsi l'enveloppe de puissance. iDRAC6 augmente uniquement sa demande de consommation énergétique potentielle maximale auprès de CMC. Il ne demande pas une diminution de sa consommation énergétique potentielle minimale si la consommation diminue.

Le CMC récupère toute puissance non utilisée auprès des serveurs à priorité inférieure et alloue ensuite cette puissance récupérée à un module d'infrastructure ou serveur à priorité supérieure.

Si la puissance allouée n'est pas suffisante, le serveur lame ne se met pas sous tension. Si la puissance allouée à la lame n'est pas suffisante, iDRAC met le système sous tension.

iDRAC6 prend également en charge l'allocation de puissance aux cartes d'extension PCIe pour les plateformes concernées. Vous pouvez modifier la puissance allouée aux cartes d'extension PCIe installées dans le logement d'extension du serveur. Deux cartes PCIe peuvent être installées sur les plateformes concernées. iDRAC ajuste de manière dynamique l'enveloppe de puissance aux exigences réelles du système pour la lame, ajoute la puissance allouée au logement de carte d'extension et demande la puissance combinée au CMC. Pour plus d'informations sur les cartes d'extension, consultez le *Manuel du propriétaire du matériel* disponible sur le site du support de Dell à l'adresse support.dell.com/manuals. Pour des informations sur la modification de l'allocation de puissance PCIe, consultez [Affichage et modification de l'allocation de puissance PCIe](#).

Une fois la lame sous tension, le BIOS démarre et détecte la consommation énergétique réelle des cartes d'extension PCIe installées. Ceci se produit au cours du POST. iDRAC conserve la valeur utilisée lors de la phase qui précède l'initialisation pour les cartes d'extension, si les deux cartes sont présentes. Une fois la valeur mise à jour obtenue d'après les cartes PCIe actuellement installées, iDRAC combine cette valeur avec la consommation énergétique estimée des cartes d'extension et signale une nouvelle valeur de puissance pour la lame globale. Si CMC n'alloue pas une puissance suffisante, iDRAC met la lame hors tension. Si CMC alloue une puissance suffisante, le BIOS est autorisé à poursuivre le démarrage et le serveur peut démarrer.

Par exemple, si 500 W est la valeur prise en considération par iDRAC avant l'initialisation, cette valeur est utilisée, excepté si vous définissez une valeur différente pour l'allocation de logement d'extension PCIe. Si vous définissez une valeur différente, cette valeur est systématiquement utilisée avant l'initialisation. La valeur est conservée tout au long des cycles d'alimentation en CA. La valeur saisie est alors comparée au nombre de cartes installées lorsque le système atteint le POST.

Affichage du bilan de puissance

Le serveur fournit des aperçus du bilan de puissance du sous-système d'alimentation à l'écran **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. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **Gestion de l'alimentation**, puis sur **Bilan de puissance**.

L'écran **Bilan de puissance** apparaît.

Le tableau **Informations du bilan de puissance** affiche les limites maximales et minimales des seuils énergétiques de la configuration système actuelle. Celles-ci couvrent la gamme des consommations en courant alternatif qu'un système à seuil soumis à une lourde charge de travail présentera au centre de données.

- 1 **Consommation de puissance potentielle minimale** représente la valeur de seuil du bilan de puissance la plus basse.
- 1 **Consommation de puissance potentielle maximale** représente la valeur de seuil du bilan de puissance la plus élevée. Cette valeur correspond également à la consommation énergétique maximale absolue de la configuration système actuelle.

Utilisation de la RACADM

Sur un serveur géré, ouvrez une interface de ligne de commande, puis entrez :

```
racadm getconfig -g cfgServerPower
```

 **REMARQUE** : Pour plus d'informations sur `cfgServerPower`, notamment les détails sur la sortie, consultez `cfgServerPower` dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Seuil du bilan de puissance

S'il est activé, le seuil du bilan de puissance applique des limites d'alimentation au système. Les performances du système sont dynamiquement ajustées afin de maintenir la consommation énergétique près du seuil spécifié.

La consommation énergétique réelle peut être inférieure pour les faibles charges de travail et peut momentanément excéder le seuil jusqu'à ce que les réglages de performances soient terminés.

 **REMARQUE** : Les informations du seuil du bilan de puissance sont en lecture seule et ne peuvent pas être activées ou configurées dans iDRAC6.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **Gestion de l'alimentation**, puis sur **Bilan de puissance**.

L'écran **Bilan de puissance** apparaît. Le tableau **Seuil du bilan de puissance** affiche les informations suivantes sur la limite de puissance du système :

- 1 **Activé** indique si le système applique le seuil du bilan de puissance.
- 1 **Seuil en watts** et **Seuil en BTU/h** affiche la limite en watts CA et en BTU/h, respectivement.
- 1 **Seuil en pourcentage (de maximum)** affiche le pourcentage de la plage de plafonnement de la puissance.

Utilisation de la RACADM

Pour afficher les données du seuil du bilan de puissance depuis la RACADM locale, sur le serveur géré, ouvrez une interface de ligne de commande et tapez :

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts
```

renvoie <valeur du plafond de puissance en watts CA>

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr
```

renvoie <valeur du plafond de puissance en BTU/h>

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent
```

renvoie <valeur du plafond de puissance en %>

 **REMARQUE :** Pour plus d'informations sur `cfgServerPower`, notamment les détails sur la sortie, consultez `cfgServerPower` dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Affichage et modification de l'allocation de puissance PCIe

L'allocation de puissance PCIe vous permet d'afficher et de modifier la puissance maximale allouée aux cartes d'extension PCIe. La puissance allouée doit être comprise entre 100 W et 500 W. L'allocation d'une puissance trop importante peut empêcher la mise sous tension de la lame ou celle d'autres lames du châssis. Si la carte d'extension PCIe consomme plus de puissance que celle allouée, la lame se mettra hors tension. Lorsque vous modifiez l'allocation de puissance PCIe, la nouvelle valeur d'allocation de puissance est utilisée au démarrage du système.

 **REMARQUE :** Les informations d'allocation de puissance PCIe ne s'appliquent pas à toutes les plateformes et ne s'afficheront pas pour les plateformes sur lesquelles elles ne s'appliquent pas.

 **REMARQUE :** Vous devez disposer des privilèges Administrateur (Configurer iDRAC et Exécuter des commandes de contrôle du serveur) pour pouvoir modifier la valeur d'allocation de puissance PCIe.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **Gestion de l'alimentation**, puis sur **Bilan de puissance**. Le tableau **Allocation de puissance PCIe** affiche l'allocation de puissance actuelle dans le champ **Seuil de puissance en watts**.
4. Saisissez une valeur requise ou cliquez sur **Valeur par défaut** pour spécifier une valeur par défaut. Les valeurs valides sont comprises entre 100 W et 500 W. La valeur par défaut est 500 W.
5. Cliquez sur **Appliquer** pour enregistrer la nouvelle valeur. La nouvelle valeur est utilisée au démarrage du système.

Utilisation de la RACADM

Pour afficher la puissance actuelle allouée aux cartes d'extension PCIe au moyen de la RACADM distante, sur le système distant, ouvrez une invite de commande et entrez la commande suivante :

```
racadm -r <idracip> -u <utilisateur> -p <mot de passe> config -g cfgServerPower -o cfgServerPowerPCIAllocation
```

Renvoie <valeur du plafond de puissance en watts CA ou BTU/h>. La valeur par défaut est 500 W.

Pour modifier la valeur d'allocation de puissance (par exemple, 250 W) :

```
racadm -r <idracip> -u <utilisateur> -p <mot de passe> config -g cfgServerPower -o cfgServerPowerPCIAllocation 250
```

Définit la valeur sur 250 W.

 **REMARQUE :** L'objet `cfgServerPowerPCIEAllocation` est pris en charge uniquement sur la RACADM distante, et non sur la RACADM locale.

 **REMARQUE :** Pour plus d'informations, consultez `cfgServerPowerPCIEAllocation` dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Contrôle de l'alimentation

iDRAC6 vous permet d'effectuer à distance une mise sous tension, une mise hors tension, une réinitialisation, un arrêt normal, une interruption non masquable (NMI) ou un cycle d'alimentation. Utilisez l'écran **Contrôle de l'alimentation** pour effectuer un arrêt méthodique avec le système d'exploitation lors des redémarrages, et des mises sous tension et hors tension.

Exécution de tâches de contrôle de l'alimentation sur un serveur

 **REMARQUE :** Vous devez disposer du privilège **Administrateur** pour effectuer des tâches de gestion de l'alimentation.

iDRAC6 vous permet d'effectuer à distance une mise sous tension, une réinitialisation, un arrêt normal, une NMI ou un cycle d'alimentation.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **Gestion de l'alimentation**.

L'écran **Contrôle de l'alimentation** apparaît.

4. Sélectionnez l'une des **opérations de contrôle de l'alimentation** suivantes en cliquant sur le bouton radio correspondant :
 - o **Allumer le système** permet de mettre le serveur sous tension (équivalent à appuyer sur le bouton d'alimentation quand le serveur est hors tension). Cette option est désactivée si le système est déjà sous tension.
 - o **Arrêter le système** permet d'éteindre le serveur. Cette option est désactivée si le système est déjà hors tension.
 - o **NMI (Interruption non masquable)** génère une NMI pour arrêter le système. Une NMI envoie une interruption de niveau élevé au système d'exploitation, qui par conséquent arrête les opérations pour permettre des activités de diagnostic ou de dépannage critiques. Cette option est désactivée si le système est déjà hors tension.
 - o **Arrêt normal** tente d'arrêter le système d'exploitation, puis met le système hors tension. L'arrêt normal nécessite que le système d'exploitation prenne en charge l'interface ACPI afin de contrôler la gestion de l'alimentation système. Cette option est désactivée si le système est déjà hors tension.
 - o **Réinitialiser le système (redémarrage à chaud)** redémarre le système sans le mettre hors tension. Cette option est désactivée si le système est déjà hors tension.
 - o **Exécuter un cycle d'alimentation sur le système (redémarrage à froid)** arrête, puis redémarre le système. Cette option est désactivée si le système est déjà hors tension.
5. Cliquez sur **Appliquer**.

Une boîte de dialogue vous demande de confirmer l'opération.
6. Cliquez sur **OK** pour exécuter la tâche de gestion d'alimentation que vous avez sélectionnée.

Utilisation de la RACADM

Pour effectuer des actions de gestion de l'alimentation à partir de la RACADM locale, entrez la commande suivante à l'invite de commande :

```
racadm serveraction <action>
```

où <action> a pour valeur `powerup`, `powerdown`, `powercycle`, `hardreset`, ou `powerstatus`.

 **REMARQUE :** Pour plus d'informations sur `serveraction`, notamment les détails sur la sortie, consultez `serveraction` dans le *Guide de référence de l'administrateur d'iDRAC6* 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](#)

Configuration et utilisation des communications série sur le LAN

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Activation des communications série sur le LAN dans le BIOS](#)
- [Configuration des communications série sur le LAN dans l'interface utilisateur Web iDRAC6](#)
- [Utilisation des communications série sur le LAN \(SOL\)](#)
- [Configuration du système d'exploitation](#)

Communications série sur le LAN (SOL) est une fonctionnalité IPMI qui permet de rediriger sur le réseau de gestion Ethernet hors bande dédié d'iDRAC6 les données de la console texte d'un serveur géré, qui seraient traditionnellement envoyées vers le port d'E/S série. La console hors bande SOL permet aux administrateurs système de gérer à distance la console texte du serveur lame depuis n'importe quel emplacement possédant un accès réseau. Les avantages des communications série sur le LAN sont les suivants :

- 1 accès à distance aux systèmes d'exploitation sans délai ;
- 1 diagnostic des systèmes hôte sur Emergency Management Services (EMS) ou Special Administrator Console (SAC) pour Windows ou dans un environnement Linux ;
- 1 visualisation de la progression d'un serveur lame pendant le POST et reconfiguration du programme de configuration du BIOS (lors de la redirection vers un port série).

Activation des communications série sur le LAN dans le BIOS

Pour configurer un serveur pour les communications série sur le LAN, vous devez suivre les étapes de configuration expliquées en détail ci-dessous :

1. Configurer les communications série sur le LAN dans le BIOS (désactivé par défaut)
2. Configurer iDRAC6 pour les communications série sur le LAN
3. Sélectionner une méthode pour initialiser les communications série sur le LAN (SSH, Telnet, proxy SOL ou IPMITool)
4. Configurer le système d'exploitation pour SOL

La communication série est **désactivée** par défaut dans le BIOS. Pour rediriger les données de la console texte hôte vers les communications série sur le LAN, vous devez activer la console virtuelle via COM1. Pour modifier le paramètre du BIOS, suivez les étapes suivantes :

1. Démarrez le serveur géré.
2. Appuyez sur <F2> pour accéder à l'utilitaire de configuration du BIOS pendant le POST.
3. Faites défiler vers le bas jusqu'à Communications série et appuyez sur <Entrée>.

Dans la fenêtre contextuelle, la liste des communications série affichée comprend les options suivantes :

- 1 Désactivé
- 1 Activé sans la console virtuelle
- 1 Activé avec la console virtuelle

Utilisez les touches fléchées pour naviguer entre les options.

4. Assurez-vous que **Activé avec la console virtuelle** est activé. Assurez-vous que l'**Adresse du port série** est COM1.
5. Assurez-vous que **Débit en bauds à sécurité intégrée** est identique au débits en bauds SOL qui est configuré sur l'iDRAC6. La valeur par défaut du débit en bauds à sécurité intégrée et du débit en bauds SOL d'iDRAC6 est 115,2 kbits/s.
6. Assurez-vous que **Redirection après démarrage** est activé. Cette option active la redirection SOL du BIOS à chaque redémarrage. Le BIOS a les valeurs **Type de terminal distant** VT100/VT220 et ANSI.
7. Enregistrez les modifications et quittez.

Le serveur géré redémarre.

Configuration des communications série sur le LAN dans l'interface utilisateur Web iDRAC6

1. Ouvrez l'écran **Configuration des communications série sur le LAN** en sélectionnant **Système**→**Accès à distance**→**iDRAC6**→**Réseau/Sécurité**→**Communications série sur le LAN**.

- Assurez-vous que l'option **Activer les communications série sur le LAN** est sélectionnée (activée). Elle est activée par défaut.
- Mettez à jour le débit en bauds SOL IPMI en sélectionnant une vitesse de données dans le menu déroulant **Débit en bauds**. Les options sont 9 600 bits/s, 19,2 kbits/s, 57,6 kbits/s et 115,2 kbits/s. La valeur par défaut est 115,2 kbits/s.
- Sélectionnez une limite de niveau de privilège pour Communications série sur le LAN.

 **REMARQUE** : Assurez-vous que le débit en bauds SOL est identique au débit en bauds à sécurité intégrée qui a été défini dans le BIOS.

- Cliquez sur **Appliquer** si vous avez apporté des modifications.

Tableau 9-1. **Communications série sur le LAN : paramètres de configuration**

Paramètre	Description
Activer les communications série sur le LAN	Lorsqu'elle est cochée, cette case indique que les communications série sur le LAN sont activées.
Débit en bauds	Indique la vitesse de transmission des données. Sélectionnez une vitesse de données de 9 600 bits/s , 19,2 kbits/s , 57,6 kbits/s ou 115,2 kbits/s .
Limite du niveau de privilège du canal	Sélectionnez une limite de niveau de privilège pour Communications série sur le LAN.

Tableau 9-2. **Boutons de configuration des communications série sur le LAN**

Bouton	Description
Imprimer	Imprime les valeurs de configuration des communications série sur le LAN qui apparaissent à l'écran.
Actualiser	Recharge l'écran Communications série sur le LAN .
Paramètres avancés	Ouvre l'écran Paramètres avancés de la configuration des communications série sur le LAN .
Appliquer	Applique les nouveaux paramètres que vous créez lors de l'affichage de l'écran Communications série sur le LAN .

- Modifiez la configuration dans l'écran **Paramètres avancés de la configuration des communications série sur le réseau local**, si nécessaire. Il est recommandé d'utiliser les valeurs par défaut. **Paramètres avancés** vous permet d'ajuster les performances SOL en modifiant les valeurs **Intervalle d'accumulation des caractères** et **Seuil d'envoi des caractères**. Pour des performances optimales, utilisez les paramètres par défaut : 10 millisecondes et 255 caractères, respectivement.

Tableau 9-3. **Paramètres avancés de la configuration des communications série sur le LAN**

Paramètre	Description
Intervalle d'accumulation des caractères	Le temps type pendant lequel l'iDRAC6 attend avant d'envoyer un paquet de données SOL partiel. Ce paramètre est spécifié en millisecondes.
Seuil d'envoi des caractères	Spécifie le nombre de caractères par paquet de données SOL. Dès que le nombre de caractères acceptés par l'iDRAC6 est supérieur ou égal à la valeur Seuil d'envoi des caractères, l'iDRAC6 commence la transmission des paquets de données SOL qui contiennent un nombre de caractères inférieur ou égal à la valeur Seuil d'envoi des caractères. Si un paquet contient un nombre de caractères inférieur à cette valeur, il est défini comme étant un paquet de données SOL partiel.

 **REMARQUE** : Si vous remplacez ces valeurs par des valeurs inférieures, les performances de la fonctionnalité de console virtuelle de SOL peuvent être diminuées. En outre, la session SOL doit attendre de recevoir un accusé de réception pour chaque paquet avant d'envoyer le paquet suivant. Les performances sont ainsi considérablement réduites.

Tableau 9-4. **Boutons des paramètres avancés de la configuration des communications série sur le LAN**

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

- Configurez SSH et Telnet pour SOL dans **Système** → **Accès à distance** → iDRAC6 → Onglet **Réseau/Sécurité** → **Services**.

 **REMARQUE** : Chaque serveur lame prend en charge une seule session SOL active.

 **REMARQUE** : Le protocole SSH est activé par défaut. Le protocole Telnet est désactivé par défaut.

8. Cliquez sur **Services** pour ouvrir l'écran **Services**.

 **REMARQUE** : Les programmes SSH et Telnet permettent d'accéder à un ordinateur distant.

9. Cliquez sur **Activé** sur **SSH** ou **Telnet**, selon les besoins.

10. Cliquez sur **Appliquer**.

 **REMARQUE** : SSH est recommandé, car il offre une sécurité accrue et des mécanismes de cryptage.

 **REMARQUE** : Une session SSH/Telnet peut durer indéfiniment pour autant que la valeur du délai d'attente est définie sur 0. La valeur du délai d'attente par défaut est 1 800 secondes.

11. Activez l'interface hors bande d'iDRAC6 (IPMI sur le LAN) en sélectionnant **Système**→**Accès à distance**→**iDRAC6**→**Réseau/Sécurité**→**Réseau**.

12. Sélectionnez l'option **Activer IPMI sur le LAN** sous **Paramètres IPMI**.

13. Cliquez sur **Appliquer**.

Utilisation des communications série sur le LAN (SOL)

Cette section indique plusieurs méthodes d'initialisation d'une session de communications série sur le LAN incluant un programme Telnet, un client SSH, IPMITool et proxy SOL. La fonctionnalité Communications série sur le LAN a pour objectif de rediriger le port série du serveur géré via iDRAC6 dans la console de votre station de gestion.

Modèle pour rediriger SOL sur Telnet ou SSH

Client Telnet (port 23)/SSH (port 22) → Connexion WAN → Serveur iDRAC6

L'implémentation SOL sur SSH/Telnet basée sur IPMI permet d'éliminer la nécessité de recourir à un utilitaire supplémentaire, car la conversion série vers le réseau se produit au sein d'iDRAC6. La console SSH ou Telnet que vous utilisez doit être capable d'interpréter les données issues du port série du serveur géré et d'y répondre. Le port série se connecte généralement à un environnement qui émule un terminal ANSI ou VT100/VT220. La console série est automatiquement redirigée vers votre console SSH ou Telnet.

Pour initier une session SOL, connectez-vous à iDRAC6 via SSH/Telnet qui vous conduit à la console de ligne de commande iDRAC6, Entrez ensuite `connect` à l'invite dollar.

Consultez [Installation de clients Telnet ou SSH](#) pour obtenir plus d'informations sur l'utilisation de clients Telnet et SSH avec iDRAC6.

Modèle pour le proxy SOL

Client Telnet (port 623) → Connexion WAN → Proxy SOL → Serveur iDRAC6

Lorsque le proxy SOL communique avec le client Telnet sur une station de gestion, il utilise le protocole TCP/IP. Le proxy SOL communique toutefois avec l'iDRAC6 du serveur géré sur le protocole RMCP/IPMI/SOL, qui est un protocole basé sur UDP. Ainsi, si vous communiquez avec l'iDRAC6 de votre système géré depuis le proxy SOL sur une connexion WAN, les performances du réseau peuvent être compromises. Le modèle d'utilisation recommandé consiste à avoir le proxy SOL et le serveur iDRAC6 sur le même LAN. La station de gestion disposant du client Telnet peut alors se connecter au proxy SOL sur une connexion WAN. Dans ce modèle d'utilisation, le proxy SOL fonctionne comme vous le souhaitez.

Modèle pour rediriger SOL sur IPMITool

IPMITool → Connexion WAN → Serveur iDRAC6

L'utilitaire SOL basé sur IPMI (IPMITool) utilise le protocole RMCP+ livré au port 623 à l'aide de datagrammes UDP. iDRAC6 exige que cette connexion RMCP+ soit cryptée. La clé de cryptage (clé KG) doit contenir des caractères zéro ou NULL qui peuvent être configurés dans l'interface utilisateur Web iDRAC6 ou dans l'utilitaire de configuration iDRAC6. Vous pouvez également effacer la clé de cryptage en appuyant sur la touche Retour arrière afin que l'iDRAC6 fournisse des caractères NULL comme clé de cryptage par défaut. RMCP+ offre comme avantage une authentification améliorée, des contrôles de l'intégrité des données, le cryptage et la capacité d'exécuter plusieurs types de charge utile. Pour plus d'informations, consultez [Utilisation de SOL sur IPMITool](#) ou le site Web IPMITool à l'adresse : <http://ipmitool.sourceforge.net/manpage.html>.

Déconnexion d'une session SOL dans la console de ligne de commande iDRAC6

Les commandes de déconnexion d'une session SOL sont orientées utilitaire. Ce n'est que lorsqu'une session SOL est complètement fermée que vous pouvez quitter l'utilitaire. Pour déconnecter une session SOL, fermez la session SOL à partir de la console de ligne de commande iDRAC6.

Lorsque vous êtes prêt à quitter la redirection SOL, appuyez sur <Entrée>, sur <Échap>, puis sur <t> (appuyez sur ces touches dans l'ordre, l'une après

l'autre). La session SOL se ferme en conséquence. La séquence Échap est également imprimée à l'écran dès qu'une session SOL est connectée. Lorsque le serveur géré est désactivé, l'établissement de la session SOL prend un peu plus de temps.

 **REMARQUE :** Si une session SOL n'est pas fermée correctement dans l'utilitaire, d'autres sessions SOL peuvent ne pas être disponibles. Pour remédier à cette situation, vous devez clôturer la console de ligne de commande dans l'interface utilisateur Web sous **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Sessions**.

Utilisation de SOL sur PuTTY

Pour démarrer SOL à partir de PuTTY sur une station de gestion Windows, suivez les étapes ci-dessous :

 **REMARQUE :** Si nécessaire, vous pouvez modifier le délai d'attente SSH/Telnet par défaut dans **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Services**.

1. Connectez-vous à l'iDRAC6 en entrant la commande suivante à l'invite de commande :

```
putty.exe [-ssh | -telnet] <nom d'ouverture de session>@<adresse-ip-iDRAC> <numéro de port>
```

 **REMARQUE :** Le numéro de port est facultatif. Il n'est requis que lorsque le port est réassigné.

2. Entrez la commande suivante à l'invite de commande pour démarrer SOL :

```
connect
```

 **REMARQUE :** Cette commande vous connecte au port série du serveur géré. Lorsqu'une session SOL est établie, la console de ligne de commande iDRAC6 n'est plus disponible. Suivez la séquence Échap correctement afin d'atteindre la console de ligne de commande iDRAC6. Quittez la session SOL à l'aide de la séquence de commandes détaillée dans [Déconnexion d'une session SOL dans la console de ligne de commande iDRAC6](#) et démarrez une nouvelle session.

 **REMARQUE :** Sous Windows, si la console EMS (Emergency Management System [système de gestion d'urgence]) est ouverte juste après un redémarrage de l'hôte, le terminal de la console SAC (Special Admin Console [console d'administration spéciale]) peut être corrompu. Quittez la session SOL comme mentionné dans [Déconnexion d'une session SOL dans la console de ligne de commande iDRAC6](#), fermez le terminal, ouvrez un autre terminal et démarrez la session SOL avec la même commande que celle décrite ci-dessus.

Utilisation de SOL sur Telnet avec Linux

Pour démarrer SOL à partir de Telnet sur une station de gestion Linux, suivez ces étapes :

 **REMARQUE :** Si nécessaire, vous pouvez modifier le délai d'attente Telnet par défaut dans **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Services**.

1. Démarrez un environnement.
2. Connectez-vous à iDRAC6 à l'aide de la commande suivante :

```
telnet <adresse-ip-iDRAC6>
```

 **REMARQUE :** Si vous avez remplacé le numéro de port par défaut (port 23) du service Telnet par un autre numéro de port, ajoutez le numéro de port à la fin de la commande Telnet.

3. Entrez la commande suivante à l'invite de commande pour démarrer SOL :

```
connect
```

4. Pour quitter une session SOL depuis Telnet sous Linux, appuyez sur <Ctrl>+J (appuyez sur la touche de contrôle tout en la maintenant enfoncée, appuyez sur la touche de crochet droit, puis relâchez). Une invite Telnet s'affiche. Tapez `quit` pour quitter Telnet.

Utilisation de SOL sur OpenSSH avec Linux

OpenSSH est un utilitaire open source permettant d'utiliser le protocole SSH. Pour démarrer SOL à partir de OpenSSH sur une station de gestion Linux, suivez ces étapes :

 **REMARQUE :** Si nécessaire, vous pouvez modifier le délai d'attente de la session SSH par défaut dans **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Services**.

1. Démarrez un environnement.
2. Connectez-vous à iDRAC6 à l'aide de la commande suivante :

```
ssh <adresse-ip-iDRAC6> -l <nom d'ouverture de session>
```

- Entrez la commande suivante à l'invite de commande pour démarrer SOL :

```
connect
```

 **REMARQUE :** Cette commande vous connecte au port série du serveur géré. Lorsqu'une session SOL est établie, la console de ligne de commande iDRAC6 n'est plus disponible. Suivez la séquence Échap correctement afin d'atteindre la console de ligne de commande iDRAC6. Quittez la session SOL (consultez [Déconnexion d'une session SOL dans la console de ligne de commande iDRAC6](#) pour fermer une session SOL active).

Utilisation de SOL sur IPMI tool

Le DVD *Dell Systems Management Tools and Documentation* fournit IPMITool, qui peut être installé sur divers systèmes d'exploitation. Consultez le *Guide d'installation rapide du logiciel* pour obtenir plus d'informations sur l'installation. Pour démarrer SOL avec IPMITool sur une station de gestion, suivez les étapes ci-dessous :

 **REMARQUE :** Si nécessaire, vous pouvez modifier le délai d'attente SOL par défaut dans **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Services**.

- Localisez le fichier **IPMITool.exe** dans le répertoire approprié.

Le chemin par défaut dans les systèmes d'exploitation Windows 32 bits est C:\Program Files\Dell\SysMgt\bmc et C:\Program Files (x86)\Dell\SysMgt\bmc dans les systèmes d'exploitation Windows 64 bits.

- Assurez-vous que la **Clé de cryptage** ne comprend que des zéros dans **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Réseau** → **Paramètres IPMI**.

- Entrez la commande suivante dans l'invite de commande Windows ou dans l'invite d'environnement Linux pour démarrer SOL via l'iDRAC :

```
ipmitool -H <adresse-ip-iDRAC> -I lanplus -U <nom d'ouverture de session> -P <mot de passe d'ouverture de session> sol activate
```

Cette commande vous connecte au port série du serveur géré.

- Pour quitter une session SOL depuis IPMITool, appuyez sur <~> et sur <.> (appuyez sur la touche tilde et sur la touche point dans l'ordre, l'une après l'autre). Essayez à plusieurs reprises car il se peut que l'iDRAC6 soit trop occupé pour accepter les touches. La session SOL se ferme.

 **REMARQUE :** Si un utilisateur ne termine pas la session SOL correctement, entrez la commande suivante pour redémarrer l'iDRAC. Veuillez laisser jusqu'à 2 minutes à l'iDRAC6 pour terminer son démarrage. Pour plus de détails, consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

```
racadm racreset
```

Ouverture de SOL avec le proxy SOL

Le proxy des communications série sur le LAN (proxy SOL) est un démon Telnet qui permet une administration basée sur LAN des systèmes distants à l'aide des protocoles de communications série sur le LAN (SOL) et IPMI. Toute application client Telnet standard, comme HyperTerminal sous Microsoft Windows ou Telnet sous Linux, peut servir à accéder aux fonctionnalités du démon. Le SOL peut être utilisé dans le mode de menu ou le mode de commande. Le protocole SOL couplé à la console virtuelle du BIOS du système distant permet aux administrateurs d'afficher et de modifier à distance les paramètres du BIOS d'un système géré sur un réseau local. La console série Linux et les interfaces EMS/SAC de Microsoft sont également accessibles via le LAN à l'aide des communications SOL.

 **REMARQUE :** Toutes les versions du système d'exploitation Windows comprennent le logiciel d'émulation de terminal HyperTerminal. Cependant, la version incluse ne fournit pas beaucoup de fonctions requises pendant l'exécution de la console virtuelle. 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 console virtuelle sur votre système est Hilgraeve HyperTerminal Private Edition 6.1 ou version ultérieure. En outre, l'utilisation de la fenêtre de ligne de commande pour effectuer une console virtuelle série Telnet risque d'afficher des caractères parasites.

 **REMARQUE :** Consultez le Guide d'utilisation de votre système pour obtenir des informations supplémentaires sur la console virtuelle, y compris les spécifications matérielles et logicielles ainsi que des instructions pour configurer les systèmes hôtes et clients afin d'utiliser la console virtuelle.

 **REMARQUE :** Les paramètres HyperTerminal et Telnet doivent être cohérents avec ceux du système géré. Par exemple, les modes Débits en bauds et Terminal doivent correspondre.

 **REMARQUE :** La commande `telnet` de Windows exécutée à partir d'une invite MS-DOS prend en charge l'émulation de terminal ANSI et le BIOS doit être configuré pour l'émulation ANSI pour afficher correctement tous les écrans.

Avant d'utiliser le proxy SOL

Avant d'utiliser le proxy SOL, consultez le *Guide d'utilisation des utilitaires du contrôleur de gestion de la carte mère* pour apprendre à configurer vos stations de gestion. Par défaut, les utilitaires de gestion du contrôleur BMC sont installés dans le répertoire suivant sur les systèmes d'exploitation Windows :

C:\Program Files\Dell\SysMgt\bmc : (système d'exploitation 32 bits)

C:\Program Files (x86)\Dell\SysMgt\bmc : (système d'exploitation 64 bits)

Le programme d'installation copie les fichiers dans les emplacements suivants sur les systèmes d'exploitation Linux Enterprise :

```
/etc/init.d/SOLPROXY.cfg
```

```
/etc/SOLPROXY.cfg
/usr/sbin/dsm_bmu_solproxy32d
/usr/sbin/solconfig
/usr/sbin/ipmish
```

Initiation de la session du proxy SOL

Pour Windows 2003

Pour démarrer le service Proxy SOL sur un système Windows après l'installation, vous pouvez redémarrer le système (le proxy SOL démarre automatiquement sur un redémarrage). Sinon, vous pouvez démarrer le service Proxy SOL manuellement en effectuant les étapes suivantes :

1. Cliquez-droite sur **Poste de travail** et cliquez sur **Gérer**.
La fenêtre **Gestion de l'ordinateur** s'affiche.
2. Cliquez sur **Services et applications**, puis sur **Services**.
Les services disponibles sont affichés sur la droite.
3. Localisez **DSM _BMU_SOLProxy** dans la liste des services et cliquez- droite pour **démarrer le service**.

En fonction de la console que vous utilisez, il y a différentes étapes pour accéder au proxy SOL. Tout au long de cette section, la station de gestion où le proxy SOL s'exécute est appelée serveur proxy SOL.

Pour Linux

Le serveur proxy SOL démarre automatiquement pendant le démarrage du système. Vous pouvez également aller dans le répertoire `/etc/init.d` et utiliser les commandes suivantes pour gérer le service Proxy SOL :

```
solproxy status
dsm_bmu_solproxy32d start
dsm_bmu_solproxy32d stop
solproxy restart
```

Utilisation de Telnet avec le proxy SOL

Ceci part du principe que le service Proxy SOL est déjà en cours d'exécution sur la station de gestion.

Pour Windows 2003 :

1. Ouvrez une fenêtre d'invite de commande sur votre station de gestion.
2. Entrez la commande `telnet` dans la ligne de commande et indiquez `localhost` comme adresse IP si le serveur proxy SOL s'exécute sur le même système et le numéro de port que vous avez spécifié lors de l'installation du proxy SOL (la valeur par défaut est 623). Par exemple :

```
telnet localhost 623
```

Pour Linux :

1. Ouvrez un environnement Linux sur votre station de gestion.
2. Entrez la commande `telnet` et indiquez `localhost` comme adresse IP du serveur proxy SOL et le numéro de port que vous avez spécifié lors de l'installation du proxy SOL (la valeur par défaut est 623). Par exemple :

```
telnet localhost 623
```

 **REMARQUE :** Que votre système d'exploitation hôte soit Windows ou Linux, si le serveur proxy SOL s'exécute sur un système différent de celui de votre station de gestion, saisissez l'adresse IP du serveur proxy SOL au lieu de localhost.

telnet <adresse IP du serveur proxy SOL> 623

Utilisation de HyperTerminal avec le proxy SOL

1. Depuis la station distante, ouvrez **HyperTerminal.exe**.
2. Choisissez **TCPIP(Winsock)**.
3. Entrez l'adresse hôte localhost et le numéro de port 623.

Connexion au contrôleur BMC du système géré distant

Lorsqu'une session du proxy SOL a été établie correctement, les choix suivants s'offrent à vous :

1. Connect to the Remote Server's BMC (Se connecter au contrôleur BMC du serveur distant)
2. Configure the Serial-Over-LAN for the Remote Server (Configurer les communications série sur le LAN pour le serveur distant)
3. Activate Virtual Console (Activer la console virtuelle)
4. Reboot and Activate Virtual Console (Redémarrer et activer la console virtuelle)
5. Help (Aide)
6. Exit (Quitter)

 **REMARQUE** : Tandis que plusieurs sessions SOL peuvent être actives en même temps, une seule session de console virtuelle peut être active à la fois pour un système géré.

 **REMARQUE** : Pour quitter une session SOL active, utilisez la séquence de caractères <~><.> Cette séquence termine SOL et vous renvoie au menu supérieur.

1. Sélectionnez l'option 1 du menu principal.
2. Entrez l'Adresse IP d'iDRAC6 du système géré distant.
3. Spécifiez le nom d'utilisateur et le mot de passe de l'iDRAC6 pour l'iDRAC6 du système géré. Le nom d'utilisateur et le mot de passe de l'iDRAC6 doivent être attribués et stockés dans le stockage rémanent de l'iDRAC6.

 **REMARQUE** : Une seule session de console virtuelle SOL avec iDRAC6 est autorisée à la fois.

 **REMARQUE** : Si nécessaire, prolongez la durée de la session SOL à l'infini en définissant la valeur du **Délai d'attente** Telnet sur zéro dans l'interface utilisateur Web iDRAC6 sous **Système**→ **Accès à distance**→ iDRAC6→ **Réseau/Sécurité**→ **Services**.

4. Fournissez la clé de cryptage IPMI si elle a été configurée dans iDRAC6.

 **REMARQUE** : Vous pouvez localiser la clé de cryptage IPMI dans l'interface utilisateur iDRAC6 dans **Système**→ **Accès à distance**→ iDRAC6→ **Réseau/Sécurité**→ **Réseau**→ **Paramètres IPMI**→ **Clé de cryptage**.

 **REMARQUE** : La clé de cryptage IPMI par défaut ne comprend que des zéros. Si vous appuyez sur <Entrée> pour l'option de cryptage, l'iDRAC6 utilise cette clé de cryptage par défaut.

5. Sélectionnez **Configurer les communications série sur le LAN pour le serveur distant** (option 2) dans le menu principal.

Le menu de configuration des communications SOL apparaît. En fonction de la condition SOL actuelle, le contenu du menu de configuration des communications SOL varie :

- 1 Si les communications SOL sont déjà activées, les paramètres actuels s'affichent, et trois choix s'offrent à vous :

1. Disable Serial-Over-LAN (Désactiver les communications série sur le LAN)
2. Change Serial-Over-LAN settings (Modifier les paramètres Communications série sur le LAN)
3. Cancel (Annuler)

- 1 Si SOL est activé, vérifiez que le débit en bauds est cohérent avec celui d'iDRAC6 et que l'utilisateur possède des privilèges d'administrateur.

- 1 Si SOL est actuellement désactivé, tapez Y pour activer SOL ou N pour laisser SOL désactivé.

- 1 Sélectionnez **Activer la console virtuelle** (option 3) dans le menu principal.

La console texte du système géré distant est redirigée vers votre station de gestion.

7. Sélectionnez **Redémarrer et activer la console virtuelle** (option 4) dans le menu principal (facultatif).

L'état de l'alimentation du système géré distant est confirmé. S'il est sous tension, vous êtes invité à choisir entre un arrêt normal et un arrêt forcé.

L'état de l'alimentation est contrôlé jusqu'à ce qu'il soit **actif**. L'exécution de la console virtuelle commence et la console texte du système géré distant est redirigée vers votre station de gestion.

Tandis que le système géré redémarre, vous pouvez accéder au programme de configuration du système BIOS pour afficher ou configurer des paramètres BIOS.

8. Sélectionnez **Aide** (option 5) dans le menu principal pour afficher une description détaillée pour chaque option.
9. Sélectionnez **Quitter** (option 6) dans le menu principal pour mettre fin à votre session Telnet et vous déconnecter du proxy SOL.

 **REMARQUE :** Si un utilisateur ne termine pas la session SOL correctement, tapez la commande suivante pour redémarrer l'iDRAC. Veuillez laisser 1 à 2 minutes à l'iDRAC6 pour terminer son démarrage. Pour plus de détails, consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

```
racadm racreset
```

Configuration du système d'exploitation

Effectuez les étapes ci-dessous pour configurer les systèmes d'exploitation génériques de type UNIX. Cette configuration est basée sur les installations par défaut de Red Hat Enterprise Linux 5.0, de SUSE Linux Enterprise Server 10 SP1 et de Windows 2003 Enterprise.

Système d'exploitation Linux Enterprise

1. Modifiez le fichier `/etc/inittab` pour activer le contrôle du débit matériel et autoriser les utilisateurs à ouvrir une session via la console SOL. Ajoutez la ligne ci-dessous à la fin de la section `#Run gettys in standard runlevels`.

```
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
```

Exemple de `/etc/inittab` original :

```
#
# inittab This file describes how the INIT process should set up (Ce fichier décrit comment le processus INIT doit configurer)
# the system in a certain run-level. (le système sur un certain niveau d'exécution).
#
SKIP this part of file (IGNOREZ cette partie du fichier)
# Run gettys in standard runlevels (Exécutez gettys aux niveaux d'exécution standard)
1:2345:respawn:/sbin/miagetty ttyl
2:2345:respawn:/sbin/miagetty ttyl
3:2345:respawn:/sbin/miagetty ttyl
4:2345:respawn:/sbin/miagetty ttyl
5:2345:respawn:/sbin/miagetty ttyl
6:2345:respawn:/sbin/miagetty ttyl
# Run gettys in standard runlevels (Exécutez xdm au niveau d'exécution 5)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Exemple de `/etc/inittab` modifié :

```
#
# inittab This file describes how the INIT process should set up (Ce fichier décrit comment le processus INIT doit configurer )
# the system in a certain run-level. (le système sur un certain niveau d'exécution).
```

```
#
SKIP this part of file (IGNOREZ cette partie du fichier)

# Run gettys in standard runlevels (Exécutez gettys aux niveaux d'exécution standard)
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1
7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Run xdm in runlevel 5 (Exécutez xdm au niveau d'exécution 5)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

2. Modifiez le fichier `/etc/securetty` pour permettre aux utilisateurs d'ouvrir une session en tant qu'utilisateur root via la console SOL. Ajoutez la ligne suivante après console :

```
ttyS0
```

Exemple de `/etc/securetty` original :

```
console
vc/1
vc/2
vc/3
vc/4
SKIP the rest of file (IGNOREZ le reste du fichier)
```

Exemple de `/etc/securetty` modifié :

```
Console
ttyS0
vc/1
vc/2
vc/3
vc/4
SKIP the rest of file (IGNOREZ le reste du fichier)
```

3. Modifiez le fichier `/boot/grub/grub.conf` ou `/boot/grub/menu.list` pour ajouter des options de démarrage pour SOL :

- e. Commentez les lignes d'affichage graphique dans les divers systèmes d'exploitation de type UNIX :

- o `splashimage=(hd0,0)/grub/splash.xpm.gz` dans RHEL 5

- o `gfxmenu (hda0,5)/boot/message` dans SLES 10

- f. Ajoutez la ligne suivante avant la première ligne `title= ...` :

```
# Redirect OS boot via SOL
```

- g. Ajoutez l'entrée suivante à la première ligne `title= ...` :

SOL redirection

- h. Ajoutez le texte suivant à la ligne `kernel/...` de la première ligne `title= ...` :

```
console=tty1 console=ttyS0,115200
```

 **REMARQUE :** `/boot/grub/grub.conf` dans Red Hat Enterprise Linux 5 est un lien symbolique vers `/boot/grub/menu.list`. Vous pouvez modifier les paramètres dans l'un d'eux.

Exemple de paramètre `/boot/grub/grub.conf` original dans RHEL 5 :

```
# grub.conf generated by anaconda (grub.conf généré par anaconda)
#
# Note that you do not have to return grub after making changes to this (Notez que vous n'avez pas besoin de réexécuter le grub après
avoir apporté des modifications à ce)
# file (fichier)
# NOTICE: You have a /boot partition. This means that (AVIS : Vous avez une partition /boot. Cela signifie que)
# all kernel and initrd paths are relative to /boot/, eg. (tous les chemins du noyau et initrd sont relatifs à /boot/, par exemple)
# root (hd0,0)
# kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol100
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu
title Red Hat Enterprise Linux 5
root (hd0,0)
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol100 rhgb quiet
initrd /initrd-2.6.18-8.el5.img
```

Exemple de `/boot/grub/grub.conf` modifié :

```
# grub.conf generated by anaconda (grub.conf généré par anaconda)
#
# Note that you do not have to return grub after making changes to this (Notez que vous n'avez pas besoin de réexécuter le grub après
avoir apporté des modifications à ce )
# file (fichier)
# NOTICE: You have a /boot partition. This means that (AVIS : Vous avez une partition /boot. Cela signifie que)
# all kernel and initrd paths are relative to /boot/, eg. (tous les chemins du noyau et initrd sont relatifs à /boot/, par exemple)
# root (hd0,0)
# kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol100
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=5
#splashimage=(hd0,0)/grub/splash.xpm/gz
```

```
hiddenmenu

# Redirect the OS boot via SOL (Redirigez le démarrage du SE via SOL)

title Redirection SOL Red Hat Enterprise Linux 5

root (hd0,0)

kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet console=tty1 console=ttyS0,115200

initrd /initrd-2.6.18-8.el5.img
```

Exemple de `/boot/grub/menu.list` original dans SLES 10 :

```
# Modified by YaST2. Last modification on Sat Oct 11 21:52:09 UTC 2008 (Modifié par YaST2. Dernière modification le sam 11 oct 21:52:09
UTC 2008)

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message

### Don't change this comment - YaST2 identifier: Original name: linux (Ne modifiez pas ce commentaire - Identificateur YaST2 : nom
d'origine : linux)###

title SUSE Linux Enterprise Server 10 SP1

root (hd0,5)

kernel /boot/vmlinuz-2.6.16-46-0.12-bigsmpt root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

initrd /boot/initrd-2.6.16.46-0.12-bigsmpt
```

Exemple de `/boot/grub/menu.list` modifié dans SLES 10 :

```
# Modified by YaST2. Last modification on Sat Oct 11 21:52:09 (Modifié par YaST2. Dernière modification le sam 11 oct 21:52:09 UTC 2008)
UTC 2008

Default 0

Timeout 8

#gfxmenu (hd0.5)/boot/message

### Don't change this comment - YaST2 identifier: Original name: linux (Ne modifiez pas ce commentaire - Identificateur YaST2 : nom
d'origine : linux)###

title SUSE Linux Enterprise Server 10 SP1 Redirection SOL

root (hd0,5)

kernel /boot/vmlinuz-2.6.16-46-0.12-bigsmpt root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts console=tty1
console=ttyS0,115200

initrd /boot/initrd-2.6.16.46-0.12-bigsmpt
```

Windows 2003 Enterprise

1. Déterminez la référence de l'entrée de démarrage en saisissant `bootcfg` dans l'invite de commande Windows. Localisez la référence de l'entrée de démarrage pour la section avec le nom convivial du système d'exploitation Windows Server 2003 Enterprise. Appuyez sur <Entrée> pour afficher les options de démarrage sur la station de gestion.
2. Activez EMS à une invite de commande Windows en entrant :

```
bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <référence de démarrage>
```

 **REMARQUE :** <référence de démarrage> correspond à la référence de l'entrée de démarrage de l'étape 1.

3. Appuyez sur <Entrée> pour vérifier que le paramètre de la console EMS est effectif.

Exemple de paramètre bootcfg original :

```
Boot Loader Settings
-----timeout:30

default:multi(0) disk (0)rdisk (0)partition (1)\WINDOWS

Boot Entries
-----

Boot entry ID: 1

Os Friendly Name: Winodws Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

Exemple de paramètre bootcfg modifié :

```
Boot Loader Settings
-----

timeout: 30

default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

redirectc : COM1

redirectbaudrate:115200

Boot Entries
-----

Boot entry ID: 1

Os Friendly Name: Windows Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation de la console virtuelle de l'interface utilisateur

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Présentation](#)
- [Utilisation de la console virtuelle](#)
- [Utilisation de Video Viewer](#)
- [Lancement de la console virtuelle et du média virtuel à distance](#)
- [Questions les plus fréquentes](#)

Cette section fournit des informations sur l'utilisation de la fonctionnalité Console virtuelle d'iDRAC6.

Présentation

La fonctionnalité Console virtuelle d'iDRAC6 vous permet d'accéder à distance aux consoles locales en mode texte ou graphique, ce qui vous permet de contrôler un ou plusieurs systèmes iDRAC6 à partir d'un emplacement unique.

Utilisation de la console virtuelle

L'écran **Console virtuelle** 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 console virtuelle :

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

Si un deuxième utilisateur demande une session de console virtuelle, le premier utilisateur en est averti et a la possibilité de refuser l'accès, d'autoriser uniquement la vidéo ou d'autoriser un accès partagé total. Le deuxième utilisateur est averti qu'un autre utilisateur contrôle la session. Le premier utilisateur doit répondre dans les trente secondes ou sinon l'accès ne sera pas accordé au deuxième utilisateur. Pendant toute la durée où deux sessions sont actives simultanément, le premier utilisateur voit un message en haut à droite de l'écran qui identifie que le deuxième utilisateur a une session active.

Si ni le premier ni le deuxième utilisateur ne possèdent de privilèges d'administrateur, la fin de la session active du premier utilisateur entraîne automatiquement la fin de la session du deuxième utilisateur.

Effacer la mémoire cache de votre navigateur

Si vous rencontrez des problèmes lors de l'utilisation de la console virtuelle (erreurs hors plage, problèmes de synchronisation, etc.), effacez la mémoire cache du navigateur pour supprimer les anciennes versions du visualiseur qui sont susceptibles d'être stockées sur le système, puis réessayez.

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 ayant 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`
2. Le **visualiseur du cache Java** apparaît.
3. Supprimez l'élément intitulé *Client de console virtuelle d'iDRAC6 et JViewer*.

Vous pouvez également exécuter `javaws -uninstall` à l'invite de commande pour effacer toutes les applications de la mémoire cache.

Résolutions d'écran prises en charge et taux de rafraîchissement

[Tableau 10-1](#) énumère les résolutions d'écran prises en charge et les taux de rafraîchissement correspondants pour une session de console virtuelle qui s'exécute sur le serveur géré.

Tableau 10-1. Résolutions d'écran prises en charge et taux de rafraîchissement

Résolution d'écran	Taux de rafraîchissement (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Configuration de la station de gestion

Pour utiliser la console virtuelle sur la station de gestion, procédez comme suit :

1. Installez et configurez un navigateur Web pris en charge. Consultez [Navigateurs Web pris en charge](#) et [Configuration d'un navigateur Web pris en charge](#).
2. Si vous utilisez Firefox ou souhaitez utiliser le visualiseur Java avec Internet Explorer, installez un environnement d'exécution Java (JRE). Consultez [Installation d'un environnement d'exécution Java \(JRE\)](#).
3. Il est recommandé de configurer la résolution d'affichage de votre moniteur sur 1280 x 1024 pixels.

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

4. Si vous utilisez Internet Explorer pour lancer une session de console virtuelle avec le plug-in Java, procédez comme suit :

- a. Dans Internet Explorer, accédez à **Outils** → **Options Internet** → **Sécurité** → **Sites de confiance** → **Personnaliser le niveau**.

 **REMARQUE :** Pour Windows 7 64 bits, cliquez sur **Outils** → **Options Internet** → **Sécurité** → **Internet** → **Personnaliser le niveau**.

- b. Dans la fenêtre **Paramètres de sécurité**, sélectionnez l'option **Désactivé** pour **Demander confirmation pour les téléchargements de fichiers**.
- c. Cliquez sur **OK** une première fois, puis une seconde fois.

Configuration de la console virtuelle et du média virtuel dans l'interface Web iDRAC6

Pour configurer la console virtuelle dans l'interface Web iDRAC6, suivez les étapes suivantes :

1. Cliquez sur **Système**, puis sur l'onglet **Console virtuelle/Média virtuel**.
2. Cliquez sur **Configuration** pour ouvrir l'écran **Configuration**.
3. Configurez les propriétés de la console virtuelle. [Tableau 10-2](#) décrit les paramètres de la console virtuelle.
4. Lorsque vous avez terminé, cliquez sur **Appliquer**.

5. Cliquez sur le bouton approprié pour continuer. Consultez [Tableau 10-3](#).

Tableau 10-2. Propriétés de configuration de la console virtuelle

Propriété	Description
Activé	Sélectionnez pour activer ou désactiver la console virtuelle. Sélectionné indique que la console virtuelle est activée. Désélectionné indique que la console virtuelle est désactivée. Activé est sélectionné par défaut.
Nombre maximal de sessions	Affiche le nombre maximal de sessions de console virtuelle possibles, 1 ou 2. Utilisez le menu déroulant pour modifier le nombre maximal de sessions de console virtuelle autorisées. Le nombre maximal par défaut est 2.
Sessions actives	Affiche le nombre de sessions de consoles actives. Ce champ est en lecture seule.
Numéro de port de clavier et de souris	Numéro de port réseau utilisé en vue de la connexion à l'option Clavier/Souris de la console virtuelle. 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 5 900 .
Numéro de port vidéo	Numéro de port réseau utilisé en vue de la connexion au service de l'écran de console virtuelle. Vous devrez peut-être modifier ce paramètre si un autre programme utilise le port par défaut. Le port par défaut est 5 901 .
Cryptage vidéo activé	Coché indique que le cryptage vidéo est activé. Tout le trafic à destination du port vidéo est crypté. Décoché indique que le cryptage vidéo est désactivé. Le trafic à destination du port vidéo n'est pas crypté. La valeur par défaut est Crypté. La désactivation du cryptage peut améliorer les performances sur les réseaux plus lents.
Mode souris	Sélectionnez Windows si le serveur géré fonctionne sous un système d'exploitation Windows. Sélectionnez Linux si le serveur géré fonctionne sous Linux. Sélectionnez USC/Diags si votre serveur ne fonctionne pas sous un système d'exploitation Windows ou Linux. REMARQUE : Vous devez sélectionner USC/Diags dans HyperV, Dell Diagnostics ou USC (services système). Le système d'exploitation par défaut est Windows .
Type de plug-in de console pour IE	Lorsque vous utilisez Internet Explorer sur un système d'exploitation Windows, vous pouvez sélectionner l'un des visualiseurs suivants : ActiveX : le visualiseur de console virtuelle <i>ActiveX</i> Java : le visualiseur de console virtuelle <i>Java</i> REMARQUE : Selon votre version d'Internet Explorer, vous devrez peut-être désactiver des restrictions de sécurité supplémentaires (consultez Configuration et utilisation du média virtuel). REMARQUE : L'environnement d'exécution Java doit être installé sur votre système client pour pouvoir utiliser le visualiseur Java.
Vidéo locale du serveur activée	Sélectionné indique que la sortie vers le moniteur de la console virtuelle est activé lors de la session de console virtuelle. Désélectionné indique que les tâches que vous effectuez avec la console virtuelle ne sont pas visibles sur le moniteur local du serveur géré.

 **REMARQUE :** Pour obtenir des informations sur l'utilisation du média virtuel avec la console virtuelle, consultez [Configuration et utilisation du média virtuel](#).

Les boutons répertoriés dans [Tableau 10-5](#) sont disponibles dans l'écran Configuration de la console virtuelle.

Tableau 10-3. Boutons de configuration de la console virtuelle

Bouton	Définition
Imprimer	Imprime l'écran Configuration
Actualiser	Recharge l'écran Configuration
Appliquer	Enregistre les nouveaux paramètres de la console virtuelle

Ouverture d'une session de console virtuelle

Lorsque vous ouvrez une session de console virtuelle, l'application de visualiseur de console virtuelle de Dell (**iDRACView**) démarre et le bureau du système distant apparaît dans le visualiseur. Grâce à **iDRACView**, 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 la console virtuelle depuis une station de gestion Windows Vista peut faire apparaître des messages liés au redémarrage de la console virtuelle. Pour éviter ce problème, définissez les valeurs du délai d'expiration appropriées aux emplacements suivants : **Panneau de configuration**→Options d'alimentation→**Economiseur d'énergie**→**Paramètres avancés**→ **Disque dur**→ **Eteindre le disque dur après <délai_d'expiration>** et dans le **Panneau de configuration**→ Options d'alimentation→ Haute performance→ **Paramètres avancés**→ **Disque dur**→ **Eteindre le disque dur après <délai_d'expiration>**.

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

1. Cliquez sur **Système**→ Onglet **Console virtuelle/Média virtuel**→ **Console virtuelle et média virtuel**.
2. Dans l'écran **Console virtuelle et média virtuel**, utilisez les informations fournies dans [Tableau 10-4](#) pour garantir qu'une session de console virtuelle est disponible.

Pour reconfigurer les valeurs des propriétés affichées, consultez [Configuration de la console virtuelle et du média virtuel dans l'interface Web iDRAC6](#).

Tableau 10-4. Informations sur la console virtuelle

Propriété	Description
Console virtuelle activée	Oui/Non
Cryptage vidéo activé	Oui/Non
Nombre maximal de sessions	Affiche le nombre maximal de sessions de console virtuelle prises en charge.
Sessions actives	Affiche le nombre actuel de sessions de console virtuelle actives.
Mode souris	Affiche le type d'accélération de la souris actif. Le mode souris doit être sélectionné selon le type de système d'exploitation installé sur le serveur géré.
Type de plug-in de console	Indique le type de plug-in configuré. ActiveX : un visualiseur Active-X est lancé. Le visualiseur Active-X fonctionne uniquement sur Internet Explorer pendant une exécution sous un système d'exploitation Windows. Java : un visualiseur Java est lancé. Le visualiseur Java peut être utilisé sur tous les navigateurs, y compris Internet Explorer. Si votre client ne s'exécute pas sur un système d'exploitation Windows, vous devez alors utiliser le visualiseur Java. Si vous accédez à iDRAC6 via Internet Explorer sous un système d'exploitation Windows, vous pouvez sélectionner Active-X ou Java comme type de plug-in. REMARQUE : La console virtuelle peut ne pas se lancer la première fois avec Internet Explorer 8 si Java est défini comme type de plug-in.
Vidéo locale du serveur activée	Oui indique que la sortie vers le moniteur de la console virtuelle est activé lors de la session de console virtuelle. Non signifie que les tâches que vous effectuez avec la console virtuelle ne sont pas visibles sur le moniteur local du serveur géré.

 **REMARQUE :** Pour des informations sur l'utilisation du média virtuel avec la console virtuelle, consultez [Configuration et utilisation du média virtuel](#).

Les boutons répertoriés dans [Tableau 10-5](#) sont disponibles dans l'écran Console virtuelle.

Tableau 10-5. Boutons de la console virtuelle

Bouton	Définition
Actualiser	Recharge l'écran Configuration de la console virtuelle
Lancer la console virtuelle	Ouvre une session de console virtuelle sur le système distant ciblé
Imprimer	Imprime l'écran Configuration de la console virtuelle

3. Si une session de console virtuelle est disponible, cliquez sur **Lancer la console virtuelle**.

 **REMARQUE :** Plusieurs boîtes de message peuvent apparaître après le lancement de l'application. Afin d'empêcher l'accès non autorisé à l'application, vous devez naviguer au sein de ces boîtes de message pendant trois minutes maximum. Sinon, vous serez invité à relancer l'application.

 **REMARQUE :** Si une ou plusieurs fenêtres **Alerte de sécurité** apparaissent au cours des étapes suivantes, lisez les informations qu'elles contiennent et cliquez sur **Oui** pour continuer.

La station de gestion se connecte à iDRAC6 et le bureau du système distant apparaît dans iDRACView.

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

Aperçu de la console virtuelle

Avant de lancer la console virtuelle, vous pouvez afficher un aperçu de l'état de la console virtuelle dans la page **Système** → **Propriétés** → **Résumé du système**. La section **Aperçu de la console virtuelle** affiche une image illustrant l'état de la console virtuelle. L'image est automatiquement actualisée toutes les 30 secondes.

 **REMARQUE** : L'image de la console virtuelle est disponible uniquement si vous avez activé la console virtuelle.

[Tableau 10-6](#) fournit des informations sur les options disponibles.

Tableau 10-6. Options d'aperçu de la console virtuelle

Option	Description
Lancer	Cliquez sur ce bouton pour lancer la console virtuelle. Si seul Média virtuel est activé, un clic sur ce lien lance directement le média virtuel. Ce bouton est désactivé si vous ne disposez pas des privilèges Console virtuelle ou si Console virtuelle et Média virtuel sont désactivés.
Paramètres	Cliquez sur ce lien pour afficher ou modifier les paramètres de configuration de la console virtuelle dans la page Configuration de la console virtuelle/du média virtuel .
Actualiser	Cliquez sur ce bouton pour actualiser l'image affichée de la console virtuelle.

Utilisation de Video Viewer

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

 **REMARQUE** : La barre de titre de la console virtuelle affiche le nom DNS ou l'adresse IP de l'iDRAC auquel vous êtes connecté depuis la station de gestion. Si iDRAC n'a pas de nom DNS, l'adresse IP est alors affichée. Le format est le suivant :

<nom DNS / adresse IPv6 / adresse IPv4>, <Modèle>, <Numéro de logement>, User : <nom d'utilisateur>, <fps>

Video Viewer fournit divers réglages de commandes tels que le mode couleur, la synchronisation de la souris, les instantanés, les macros de clavier, les actions d'alimentation et l'accès au média virtuel. Cliquez sur **Aide** pour plus d'informations sur ces fonctions.

Lorsque vous démarrez une session de console virtuelle et que Video Viewer apparaît, vous devrez peut-être régler le mode couleur et synchroniser les pointeurs de souris.

[Tableau 10-7](#) décrit les options de menu disponibles dans le visualiseur.

Tableau 10-7. Sélections sur la barre de menus du visualiseur

Élément de menu	Élément	Description
Vidéo	Pause	Met provisoirement en pause la console virtuelle.
	Reprendre	Reprend la console virtuelle.
	Actualiser	Redessine l'image d'écran du visualiseur.
	Capturer l'écran actuel	Capture l'écran du système distant actuel dans un fichier .bmp. Une boîte de dialogue s'affiche pour que vous puissiez enregistrer le fichier dans un emplacement spécifié.
	Plein écran	Pour développer Video Viewer en mode Plein écran, cliquez en haut à droite du visualiseur pour passer en plein écran.
	Quitter	Lorsque vous avez terminé d'utiliser la console et que vous avez fermé la session (en suivant la procédure de fermeture de session du système distant), sélectionnez Quitter dans le menu Vidéo pour fermer la fenêtre Video Viewer .
Clavier	Touche Alt droite maintenue enfoncée	Sélectionnez cet élément avant de taper sur des touches que vous souhaitez combiner avec la touche <Alt> droite.
	Touche Alt gauche maintenue enfoncée	Sélectionnez cet élément avant de taper sur des touches que vous souhaitez combiner avec la touche <Alt> gauche.
	Touche Windows gauche	Sélectionnez Maintenir enfoncé avant de taper des caractères que vous souhaitez combiner avec la touche Windows gauche. Sélectionnez Appuyer et relâcher pour envoyer une séquence de touche Windows gauche.
	Touche Windows droite	Sélectionnez Maintenir enfoncé avant de taper des caractères que vous souhaitez combiner avec la touche Windows droite. Sélectionnez Appuyer et relâcher pour envoyer une séquence de touche Windows droite.
	Macros	Lorsque vous sélectionnez une macro ou saisissez son raccourci clavier, l'action s'exécute sur le système distant. Video Viewer fournit les macros suivantes : <ul style="list-style-type: none"> 1 Alt+Ctrl+Suppr 1 Alt+Tab 1 Alt+Échap 1 Ctrl+Échap 1 Alt+Espace 1 Alt+Entrée 1 Alt+Tiret 1 Alt+F4 1 ImprÉcran 1 Alt+ImprÉcran

		<ul style="list-style-type: none"> 1 F1 1 Pause 1 Alt+M 1 Alt+D 1 Alt+ImprÉcran+M 1 Alt+ImprÉcran+P
	Transfert des données clavier	Le mode de transfert des données clavier permet à toutes les fonctions clavier du client d'être redirigées vers le serveur.
Souris	Synchroniser le curseur	Synchronise le curseur pour que la souris du client soit redirigée vers la souris du serveur.
	Masquer le curseur local	Seul le curseur de la console virtuelle est affiché. Ce paramètre est recommandé lors de l'exécution d'USC dans une console virtuelle.
Options	Mode couleur	<p>Vous permet de sélectionner une profondeur de couleur pour améliorer les performances sur le réseau. Par exemple, si vous installez le logiciel à partir du média virtuel, vous pouvez choisir la profondeur de couleur la plus basse de manière à ce que moins de bande passante réseau soit utilisée par le visualiseur de console virtuelle, laissant ainsi davantage de bande passante pour le transfert des données à partir du média.</p> <p>Le mode couleur peut être défini sur couleur 15 bits et couleur 7 bits.</p>
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.
Média	Assistant Média virtuel	<p>Le menu Média donne accès à l'assistant Média virtuel, qui vous permet de vous rediriger vers un périphérique ou une image de type :</p> <ul style="list-style-type: none"> 1 Lecteur de disquette 1 CD 1 DVD 1 Image au format ISO 1 Lecteur flash USB <p>Pour des informations sur la fonctionnalité Média virtuel, consultez Configuration et utilisation du média virtuel.</p> <p>La fenêtre du visualiseur de console virtuelle doit rester active lorsque vous utilisez le média virtuel.</p>
Aide	À propos d'iDRACView	Affiche la version d'iDRACView.

Synchronisation des pointeurs de la souris

Lorsque vous vous connectez à un système Dell PowerEdge distant en utilisant la console virtuelle, la vitesse d'accélération de la souris sur le système distant peut ne pas être synchronisée avec le pointeur de la souris de votre station de gestion, provoquant l'apparition de deux pointeurs de souris dans la fenêtre Video Viewer.

Pour synchroniser les pointeurs de la souris, cliquez sur **Souris** → **Synchroniser le curseur** ou appuyez sur <Alt><M>.

L'élément de menu Synchroniser le curseur est une touche à bascule. Assurez-vous qu'une coche est insérée en regard de l'élément dans le menu, ce qui permet à la synchronisation de la souris d'être active.

Lorsque vous utilisez Red Hat Enterprise Linux ou Novell SUSE Linux, veillez à configurer le mode souris pour Linux avant de lancer le visualiseur. Consultez [Configuration de la console virtuelle et du média virtuel dans l'interface Web iDRAC6](#) pour obtenir de l'aide sur la configuration. Les paramètres de souris par défaut du système d'exploitation sont utilisés pour contrôler le curseur de la souris dans l'écran **Console virtuelle** d'iDRAC6.

Désactivation ou activation de la console locale

Vous pouvez configurer iDRAC6 pour interdire les connexions de la console virtuelle via l'interface Web iDRAC6. Lorsque la console locale est désactivée, un point de condition jaune apparaît dans la liste des serveurs (OSCAR) pour indiquer que la console est verrouillée dans iDRAC6. Lorsque la console locale est activée, le point de condition est vert.

Si vous souhaitez vous assurer que vous disposez d'un accès exclusif à la console de serveur géré, vous devez désactiver la console locale *et reconfigurer le nombre maximal de sessions* sur 1 dans l'**écran Console virtuelle**.

 **REMARQUE :** Si vous désactivez (mettez hors tension) la vidéo locale sur le serveur, le moniteur, le clavier et la souris connectés à la console virtuelle sont désactivés.

Pour désactiver ou activer la console locale, procédez comme suit :

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et connectez-vous à iDRAC6. Consultez la section [Accès à l'interface Web](#) pour plus d'informations.
2. Cliquez sur **Système**, cliquez sur l'onglet **Console virtuelle/Média virtuel**, puis sur **Configuration**.
3. Si vous souhaitez désactiver (arrêter) la vidéo locale sur le serveur, dans l'écran **Configuration**, désélectionnez l'option **Vidéo du serveur local activée**, puis cliquez sur **Appliquer**. La valeur par défaut est **Activé (case cochée)**.

- Si vous souhaitez activer (démarrer) la vidéo locale sur le serveur, dans l'écran **Configuration**, cochez la case **Vidéo du serveur local activée**, puis cliquez sur **Appliquer**.

L'écran Console virtuelle affiche la condition de la vidéo du serveur local.

Lancement de la console virtuelle et du média virtuel à distance

Vous pouvez lancer la console virtuelle ou le média virtuel en saisissant une URL unique dans un navigateur pris en charge au lieu de le lancer depuis l'interface utilisateur Web iDRAC6. Selon la configuration de votre système, vous effectuerez le processus d'authentification manuelle (page d'ouverture de session) ou vous serez dirigé vers le visualiseur de la console virtuelle ou du média virtuel (iDRACView) 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 en charge les ouvertures de session SSO, locales et AD.

Format d'URL

Si vous saisissez le lien `https://<idrac6_ip>/console` dans le navigateur, vous pourrez être invité à effectuer la procédure normale d'ouverture de session manuelle en fonction de 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 aboutit, la vue Console virtuelle ou Média virtuel n'est pas lancée. Vous serez alors redirigé vers la page d'accueil de l'interface utilisateur iDRAC6.

 **REMARQUE :** L'URL utilisée pour lancer iDRACView est sensible à la casse et doit être tapée uniquement en minuscules.

Scénarios d'erreurs généraux

[Tableau 10-8](#) répertorie les scénarios d'erreurs généraux, les causes de ces erreurs et le comportement d'iDRAC6.

Tableau 10-8. 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.	Même comportement lorsque <code>https://<ip></code> est spécifié et que l'ouverture de session échoue.
Privilèges insuffisants	Vous ne disposez pas des privilèges Console virtuelle et Média virtuel.	iDRACView ne se lance pas et vous êtes redirigé vers la page d'interface utilisateur de configuration Console virtuelle/Média virtuel.
Console virtuelle désactivée	La console virtuelle est désactivée sur votre système.	iDRACView ne se lance pas et vous êtes redirigé vers la page d'interface utilisateur de configuration Console virtuelle/Média virtuel.
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

[Tableau 10-9](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 10-9. Utilisation de la console virtuelle : Questions les plus fréquentes

Question	Réponse
La console virtuelle ne parvient pas à fermer la session lors de la fermeture de la session de l'interface utilisateur Web hors bande.	Les sessions de console virtuelle et de média virtuel demeurent actives, même si la session Web est fermée. Fermez les applications du visualiseur de média virtuel et de console virtuelle pour 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 que la requête pour activer la vidéo locale est reçue par l'iDRAC6, la vidéo est activée immédiatement.
Est-ce que l'utilisateur local peut également désactiver la vidéo ?	Oui, un utilisateur local peut utiliser la CLI RACADM locale pour désactiver la vidéo.
Est-ce que l'utilisateur local peut également activer la vidéo ?	Non. Une fois que la console locale est désactivée, le clavier et la souris de l'utilisateur local sont désactivés et ne sont plus en mesure de modifier des paramètres.
La désactivation de la vidéo locale désactive-t-elle aussi le clavier et la souris locaux ?	Oui.
La désactivation de la console locale désactive-t-elle la vidéo sur la session de la console distante ?	Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de la console distante.

Quels sont les privilèges nécessaires à un utilisateur iDRAC6 pour activer ou désactiver la vidéo locale du serveur ?	Tout utilisateur disposant de privilèges de configuration iDRAC6 peut activer ou désactiver la console locale.
Comment connaître la condition actuelle de la vidéo locale du serveur ?	La condition est affichée sur l'écran Console virtuelle et média virtuel de l'interface Web iDRAC6. La commande CLI RACADM <code>racadm getconfig -g cfgRacTuning</code> affiche la condition dans l'objet cfgRacTuneLocalServerVideo . Cette commande <code>racadm</code> peut être exécutée à partir de Telnet/SSH ou d'une session distante sur iDRAC6. La commande RACADM distante est : <code>racadm -r <ip idrac> -u <utilisateur> -p <mot de passe> getconfig -g cfgRacTuning</code> La condition est également visible dans l'affichage OSCAR de la console virtuelle. Lorsque la console locale est activée, une condition de couleur verte apparaît en regard du nom du serveur. Lorsqu'elle est désactivée, un point jaune indique que la console locale est verrouillée par iDRAC6.
Je n'arrive pas à voir le bas de l'écran système à partir de la fenêtre Console virtuelle.	Assurez-vous que la résolution du moniteur de la station de gestion est définie sur 1280 x 1024.
La fenêtre de la console est tronquée.	Le visualiseur de console virtuelle sous Linux requiert un jeu de caractères UTF-8. Vérifiez vos paramètres régionaux et réinitialisez le jeu de caractères si nécessaire. Consultez la section Configuration des paramètres régionaux sous Linux pour plus d'informations.
L'écran du serveur géré est vide lorsque je charge le système d'exploitation Windows 2000. Pourquoi ?	Le serveur géré ne dispose pas du pilote vidéo ATI qui convient. Mettez le pilote vidéo à jour.
La souris ne se synchronise pas sous DOS pendant l'exécution de la console virtuelle. Pourquoi ?	Le BIOS de Dell émule le pilote de souris comme s'il s'agissait d'une souris PS/2. La souris PS/2 est conçue pour utiliser la position relative de son pointeur, ce qui produit un délai de synchronisation. L'iDRAC6 a un pilote de souris USB, ce qui permet un positionnement absolu et un suivi plus proche du pointeur de la souris. Même si iDRAC6 transmettait la position absolue de la souris USB au BIOS Dell, l'émulation du BIOS la reconvertirait en position relative et le comportement ne changerait pas. Pour résoudre ce problème, définissez le mode souris sur USC/Diags dans l'écran Configuration .
Pourquoi la souris ne se synchronise-t-elle pas sous la console de texte Linux (dans Dell Unified Server Configurator (USC), Dell Lifecycle Controller (LC) ou Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)) ?	La console virtuelle 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 console virtuelle. Assurez-vous que Synchroniser la souris est coché dans le menu Souris . Appuyez sur <Alt><M> ou sélectionnez Souris → Synchroniser la souris pour faire activer la synchronisation de la souris. Lorsque la synchronisation est activée, une coche apparaît en regard de la sélection dans le menu Souris .
Je ne peux pas utiliser de clavier ou de souris lorsque j'installe un système d'exploitation Microsoft à distance en utilisant la console virtuelle d'iDRAC6. Pourquoi ?	Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système sur lequel la console virtuelle 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 console virtuelle dans le BIOS. Ce message est généré par Microsoft pour avertir l'utilisateur que la console virtuelle est activée. Pour que ce message n'apparaisse pas, désactivez toujours la console virtuelle 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 ?	Lorsqu'on y accède via iDRAC6, l'indicateur Verr Num sur la station de gestion ne correspond pas nécessairement à l'état du verrouillage numérique sur le serveur distant. L'état Verr Num dépend du paramètre sur le serveur distant 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 console virtuelle à partir de l'hôte local ?	Vous configurez une session de console virtuelle à partir du système local. Cette opération n'est pas prise en charge.
Si j'exécute une session de console virtuelle 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 console virtuelle ?	Il est recommandé d'utiliser une connexion de 5 Mo/s pour optimiser les performances. Une connexion de 1 Mo/s suffit pour une performance minimale.
Quelle est la configuration système minimale requise pour que ma station de gestion puisse exécuter la console virtuelle ?	La station de gestion nécessite un processeur Intel Pentium III 500 MHz avec au moins 256 Mo de RAM.
Après avoir lancé la console virtuelle, je peux utiliser la souris uniquement sur la console virtuelle, et non sur mon système local. Pourquoi cette situation se produit-elle et que dois-je faire pour pouvoir utiliser la souris sur la console virtuelle et sur mon système local ?	Cette situation se produit si Mode Souris est défini sur USC/Diags . Appuyez sur la touche rapide <Alt><M> pour utiliser la souris sur votre système local. Appuyez à nouveau sur <Alt><M> pour utiliser la souris sur la console virtuelle.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration de la carte SD vFlash et gestion des partitions vFlash

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Installation d'une carte SD vFlash ou standard](#)
- [Configuration de la carte SD vFlash ou standard à l'aide de la RACADM](#)
- [Gestion des partitions vFlash via l'interface Web iDRAC6](#)
- [Gestion des partitions vFlash à l'aide de la RACADM](#)
- [Questions les plus fréquentes](#)

La carte SD vFlash est une carte Secure Digital (SD) qui se branche dans un logement de carte iDRAC6 Enterprise en option à l'arrière du système. Son espace de stockage se comporte comme toute clé de mémoire flash USB. Il s'agit de l'emplacement de stockage des partitions définies par l'utilisateur qui peuvent être configurées pour être exposées au système en tant que périphérique USB et également pour être utilisées afin de créer un périphérique USB d'amorçage. Selon le mode d'émulation sélectionné, les partitions seront exposées au système en tant que lecteur de disquette et disque dur ou en tant que lecteur de CD/DVD. Vous pouvez configurer n'importe lequel d'entre eux comme périphérique d'amorçage.

Les cartes SD vFlash et les cartes SD standard sont prises en charge. Une *carte SD vFlash* est la carte qui prend en charge les nouvelles fonctionnalités vFlash améliorées. Une *carte SD standard* est une carte SD normale prête à l'emploi qui ne prend en charge que des fonctionnalités vFlash limitées.

La carte SD vFlash vous permet de créer jusqu'à 16 partitions. Vous pouvez attribuer un nom à la partition lorsque vous la créez, et vous pouvez effectuer toute une gamme d'opérations afin de gérer et d'utiliser les partitions. Une carte SD vFlash peut avoir n'importe quelle taille, jusqu'à 8 Go. Chaque partition peut aller jusqu'à 4 Go.

Une carte SD standard peut avoir n'importe quelle taille, mais elle ne prend en charge qu'une seule partition. La taille de la partition est limitée à 256 Mo. Le nom de la partition est VFLASH par défaut.

REMARQUE : Veillez à insérer uniquement une carte SD vFlash ou une carte SD standard dans le logement de carte iDRAC6 Enterprise. Si vous insérez une carte d'un autre format (par exemple, une carte multimédia [MMC]), le message d'erreur suivant s'affiche lorsque vous initialisez la carte : *An error has occurred while initializing SD card (Une erreur s'est produite lors de l'initialisation de la carte SD)*.

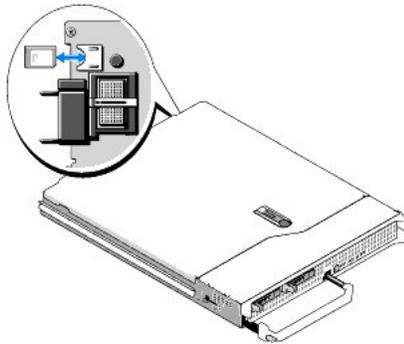
Si vous êtes un administrateur, vous pouvez effectuer toutes les opérations sur les partitions vFlash. Dans le cas contraire, vous devez disposer des privilèges Accès au média virtuel pour pouvoir créer, supprimer, formater, connecter, déconnecter ou copier le contenu de la partition.

REMARQUE : Vous ne pouvez effectuer qu'une seule opération vFlash à la fois. La première opération doit être terminée avant que vous ne commenciez une autre opération vFlash. Par exemple, si vous lancez une opération de création à partir d'une image à l'aide de la RACADM, vous ne pouvez pas effectuer d'opération de création, de téléchargement ou de formatage via la RACADM ou l'interface utilisateur. Vous devez attendre que l'opération soit terminée avant d'effectuer l'opération vFlash suivante.

Installation d'une carte SD vFlash ou standard

1. Retirez la lame du châssis.
2. Identifiez le logement de carte vFlash à l'arrière du système.

REMARQUE : Il n'est pas nécessaire de retirer le capot de la lame pour installer ou retirer la carte.



3. L'étiquette étant orientée vers le haut, insérez les broches de contact de la carte SD dans le logement correspondant du module.

REMARQUE : Le logement est muni d'un repère qui permet d'insérer la carte dans le bon sens.

4. Appuyez sur la carte pour qu'elle s'enclenche dans son logement.
5. Réinstallez la lame dans le châssis.

Retrait d'une carte SD vFlash ou standard

Pour retirer la carte SD vFlash ou standard, enfoncez-la pour la déverrouiller, puis sortez-la de son logement.

Configuration de la carte SD vFlash ou standard via l'interface Web iDRAC6

Une fois que vous avez installé la carte SD vFlash ou standard, vous pouvez afficher ses propriétés, activer ou désactiver vFlash, et initialiser la carte. La carte doit être activée pour pouvoir gérer les partitions. Lorsque la carte est désactivée, vous pouvez uniquement afficher ses propriétés. L'opération d'initialisation supprime les partitions existantes et réinitialise la carte.

 **REMARQUE :** Vous devez disposer de l'autorisation Configurer iDRAC pour pouvoir activer ou désactiver vFlash, ou initialiser la carte.

Si aucune carte n'est disponible dans le logement de carte iDRAC6 Enterprise du système, le message d'erreur suivant apparaît.

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.)

Pour afficher et configurer la carte SD vFlash ou standard :

1. Ouvrez une fenêtre de navigateur Web pris en charge et ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **vFlash**. La page **Propriétés de la carte SD** apparaît.

[Tableau 11-1](#) répertorie les propriétés affichées pour la carte SD.

Tableau 11-1. Propriétés de la carte SD

Attribut	Description
Nom	Affiche le nom de la carte installée dans le logement de carte iDRAC6 Enterprise du serveur. Si la carte prend en charge les nouvelles fonctionnalités vFlash améliorées, la mention <i>Carte SD vFlash</i> apparaît. Si elle prend en charge les fonctionnalités vFlash limitées, la mention <i>Carte SD</i> apparaît.
Taille	Affiche la taille de la carte en gigaoctets (Go).
Espace disponible	Affiche l'espace inutilisé sur la carte SD en Mo. Cet espace est disponible pour créer d'autres partitions sur la carte SD vFlash. Si la carte SD insérée n'est pas initialisée, l'espace disponible indique alors que la carte n'est pas initialisée.
Protégé contre l'écriture	Indique si la carte est protégée contre l'écriture ou non.
Intégrité	Affiche l'intégrité générale de la carte SD. Elle peut être : <ul style="list-style-type: none">1 OK1 Avertissement1 Critique Si elle est définie sur Avertissement, réinitialisez la carte. Si elle est définie sur Critique, réinstallez et réinitialisez la carte.
vFlash activé	Cochez la case pour gérer les partitions vFlash sur la carte. Décochez la case pour désactiver la gestion des partitions vFlash.

4. Cliquez sur **Appliquer** pour activer ou désactiver la gestion des partitions vFlash sur la carte.

Si une partition vFlash est connectée, vous ne pouvez pas désactiver vFlash et un message d'erreur s'affiche.

 **REMARQUE :** Si vFlash est désactivé, vous pouvez uniquement afficher les propriétés de la carte SD et vous ne pourrez pas effectuer d'autres opérations vFlash telles que la création d'une partition (vide et à l'aide d'un fichier image), la gestion des partitions, le formatage des partitions et le téléchargement du contenu d'une partition.

5. Cliquez sur **Initialiser**. Toutes les partitions existantes sont supprimées et la carte est réinitialisée. Un message de confirmation s'affiche.
6. Cliquez sur **OK**. Lorsque l'opération d'initialisation est terminée, un message de réussite s'affiche.

 **REMARQUE :** **Initialiser** est disponible uniquement si vous sélectionnez l'option **vFlash activé**.

Si une partition vFlash est connectée, l'opération d'initialisation échoue et un message d'erreur s'affiche.

Si vous cliquez sur une option quelconque sur les pages vFlash lorsqu'une application telle que le fournisseur WSMAN, l'utilitaire de configuration d'iDRAC6 ou RACADM utilise vFlash, ou bien si vous naviguez vers une autre page de l'interface utilisateur, iDRAC6 peut afficher le message suivant.

SD card is temporarily unavailable. To retry, click Refresh. (La carte SD est provisoirement indisponible. Pour réessayer, cliquez sur Actualiser).

Configuration de la carte SD vFlash ou standard à l'aide de la RACADM

Vous pouvez afficher et configurer la carte SD vFlash ou standard en utilisant les commandes RACADM depuis la console locale, distante ou Telnet/SSH.

 **REMARQUE :** Vous devez disposer de l'autorisation Configurer iDRAC pour pouvoir activer ou désactiver vFlash, et initialiser la carte.

Affichage des propriétés de la carte SD vFlash ou standard

Ouvrez une console Telnet/SSH/série sur le serveur, ouvrez une session et tapez la commande suivante :

```
racadm getconfig -g cfgvFlashSD
```

Les propriétés en lecture seule suivantes s'affichent :

```
1  cfgvFlashSDSize
1  cfgvFlashSDLicense
1  cfgvFlashSDAvailableSize
1  cfgvFlashSDHealth
```

Activation ou désactivation de la carte SD vFlash ou standard

Ouvrez une console Telnet/SSH/série sur le serveur, ouvrez une session et tapez la commande suivante :

```
1  Pour activer une carte SD vFlash ou standard :
    racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
1  Pour désactiver une carte SD vFlash ou standard :
    racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
```

 **REMARQUE :** La commande RACADM fonctionne uniquement si une carte SD vFlash ou standard est présente. Si aucune carte n'est présente, le message suivant apparaît : *ERROR: SD Card not present. (ERREUR : Carte SD non présente)* .

Initialisation de la carte SD vFlash ou standard

Ouvrez une console Telnet/SSH/série sur le serveur, ouvrez une session et tapez la commande suivante :

```
racadm vflashsd initialize
```

Toutes les partitions existantes sont supprimées et la carte est réinitialisée.

Obtention de la dernière condition sur la carte SD vFlash ou standard

Ouvrez une console Telnet/SSH/série sur le serveur, ouvrez une session et tapez la commande suivante pour obtenir la condition de la dernière commande envoyée à la carte SD vFlash ou standard :

```
racadm vFlashsd status
```

Réinitialisation de la carte SD vFlash ou standard

Ouvrez une console Telnet/SSH/série sur le serveur, ouvrez une session et tapez :

```
racadm vflashsd initialize
```

Pour plus d'informations sur vflashsd, consultez le *Guide de référence de l'administrateur d'iDRAC* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

 **REMARQUE :** La commande `racadm vmkey reset` est dépréciée à partir de la version 1.5. La fonctionnalité de cette commande est désormais couverte par `vflashsd initialize`. Alors que l'exécution de la commande `vmkey reset` aboutira, il est recommandé d'utiliser la commande `vflashsd initialize`. Pour plus d'informations, consultez [Initialisation de la carte SD vFlash ou standard](#).

Gestion des partitions vFlash via l'interface Web iDRAC6

Vous pouvez réaliser les tâches suivantes :

- 1 Créer une partition vide
- 1 Créer une partition à l'aide d'un fichier image
- 1 Formater une partition
- 1 Afficher les partitions disponibles
- 1 Modifier une partition
- 1 Connecter/Déconnecter une partition
- 1 Supprimer les partitions existantes
- 1 Télécharger le contenu d'une partition
- 1 Démarrer sur une partition

Création d'une partition vide

Une partition vide est similaire à une clé USB vide. Vous pouvez créer des partitions vides sur une carte SD vFlash ou standard. Vous pouvez choisir de créer des partitions du type *Disquette* ou *Disque dur*. La partition de type CD n'est pas prise en charge pour la création de partitions vides.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir créer des partitions vides.

Avant de créer une partition vide, assurez-vous que :

- 1 La carte est initialisée.
- 1 La carte n'est pas protégée contre l'écriture.
- 1 Une opération d'initialisation n'est pas déjà en cours sur la carte.

Pour créer une partition vFlash vide :

1. Sur l'interface Web iDRAC6, sélectionnez **Système** → onglet **vFlash** → sous-onglet **Créer une partition vide**. La page **Créer une partition vide** s'affiche.
2. Entrez les informations mentionnées dans [Tableau 11-2](#).
3. Cliquez sur **Appliquer**. Une nouvelle partition est créée.

 **REMARQUE :** Lorsqu'une création de partition est en cours, la progression ou la condition n'est pas affichée.

Un message d'erreur apparaît si :

- 1 La carte est protégée contre l'écriture.
- 1 Le nom correspond au nom d'une partition existante.
- 1 Une valeur non entière est saisie pour la taille de la partition, la valeur excède l'espace disponible sur la carte ou la taille de partition demandée est supérieure à 4 Go.
- 1 Une opération d'initialisation est déjà en cours sur la carte.

 **REMARQUE :** La nouvelle partition n'est pas formatée (RAW).

Tableau 11-2. Options de la page **Créer une partition vide**

Champ	Description
Index	Sélectionnez un index de partition. Seuls les index non utilisés sont affichés dans la liste déroulante. L'index disponible le plus bas est sélectionné par défaut. Vous pouvez le remplacer par une autre valeur d'index de la liste déroulante. REMARQUE : Pour la carte SD standard, seul l'index 1 est disponible.
Nom	Entrez un nom unique pour la nouvelle partition. Le nom peut contenir jusqu'à six caractères alphanumériques. N'incluez pas d'espace dans le nom. Les caractères sont affichés en majuscules. REMARQUE : Pour la carte SD standard, le nom doit être VFLASH. Dans le cas contraire, un message d'erreur s'affiche.
Type d'émulation	Sélectionnez le type d'émulation pour la partition dans la liste déroulante. Les options disponibles sont Disquette et Disque dur .
Taille	Entrez la taille de la partition en mégaoctets (Mo). La taille de partition maximale est 4 Go ou est inférieure ou égale à l'espace disponible sur la carte SD vFlash. REMARQUE : Pour la carte SD standard, la taille de partition peut aller jusqu'à 256 Mo.

Création d'une partition à l'aide d'un fichier image

Vous pouvez créer une nouvelle partition sur une carte SD vFlash ou standard à l'aide d'un fichier image (disponible au format **.img** ou **.iso**). Vous pouvez créer une partition de type Disquette, Disque dur ou CD. La partition créée est en lecture seule.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir créer des partitions.

La taille de la partition récemment créée est égale à celle du fichier image. La taille du fichier image doit être :

- 1 Inférieure ou égale à l'espace disponible sur la carte.
- 1 Inférieure ou égale à 4 Go. La taille de partition maximale est de 4 Go.

Avec l'interface Web, la taille de l'image pouvant être téléversée sur la carte SD vFlash est limitée à 2 Go maximum pour les navigateurs 32 bits et 64 bits (Internet Explorer et FireFox).

Avec la RACADM et l'interface WSMAN, la taille de l'image pouvant être téléversée sur une carte SD vFlash est de 4 Go maximum.

Pour la carte SD standard, la taille de l'image doit être inférieure ou égale à 256 Mo.

Avant de créer une partition à partir d'un fichier image, assurez-vous que :

- 1 La carte est initialisée.
- 1 La carte n'est pas protégée contre l'écriture.
- 1 Une opération d'initialisation n'est pas déjà en cours sur la carte.

 **REMARQUE :** Lors de la création d'une partition à partir d'un fichier image, vérifiez que le type d'image et le type d'émulation correspondent. iDRAC émule le périphérique d'après le type d'image spécifié. Des problèmes peuvent survenir lorsque l'image téléversée et le type d'émulation ne correspondent pas. Par exemple, si la partition est créée à l'aide d'une image ISO et que le type d'émulation spécifié est Disque dur, le BIOS ne sera pas en mesure de démarrer depuis cette image.

Pour créer une partition vFlash à l'aide d'un fichier image :

1. Sur l'interface Web iDRAC6, sélectionnez **Système** → onglet **vFlash** → sous-onglet **Créer à partir d'une image**. La page **Créer une partition à partir d'un fichier image** s'affiche.
2. Entrez les informations mentionnées dans [Tableau 11-3](#).
3. Cliquez sur **Appliquer**. Une nouvelle partition est créée à l'aide du fichier image.

 **REMARQUE :** Lorsqu'une création de partition est en cours, la progression ou la condition n'est pas affichée.

Un message d'erreur apparaît si :

- 1 La carte est protégée contre l'écriture.
- 1 Le nom correspond au nom d'une partition existante.
- 1 La taille du fichier image est supérieure à 4 Go ou excède l'espace disponible sur la carte.
- 1 Le fichier image n'existe pas ou l'extension du fichier image n'est ni **.img**, ni **.iso**.
- 1 Une opération d'initialisation est déjà en cours sur la carte.

Tableau 11-3. **Créer une partition à partir des options de la page Fichier image**

Champ	Description
Index	Sélectionnez un index de partition. Seuls les index non utilisés sont affichés dans la liste déroulante. L'index disponible le plus bas est sélectionné par défaut. Vous pouvez le remplacer par une autre valeur d'index de la liste déroulante. REMARQUE : Pour la carte SD standard, seul l'index 1 est disponible.
Nom	Entrez un nom unique pour la nouvelle partition. Il peut contenir jusqu'à six caractères alphanumériques. N'incluez pas d'espaces dans le nom. Les caractères sont affichés en majuscules. REMARQUE : Pour la carte SD standard, le nom doit être VFLASH. Dans le cas contraire, un message d'erreur s'affiche.
Type d'émulation	Sélectionnez le type d'émulation pour la partition dans la liste déroulante. Les options disponibles sont Disquette , Disque dur et CD-ROM .
Emplacement de l'image	Cliquez sur Parcourir et spécifiez l'emplacement du fichier image. Seuls les types de fichier .img et .iso sont pris en charge.

Formatage d'une partition

Vous pouvez formater une partition existante sur la carte SD vFlash d'après le type de système de fichiers. Les types de système de fichiers pris en charge sont EXT2, EXT3, FAT16 et FAT32. La carte SD standard avec fonctionnalités vFlash limitées ne prend en charge que le format FAT32.

Vous pouvez uniquement formater les partitions Disque dur ou Disquette. Le formatage des partitions de type CD n'est pas pris en charge. Vous ne pouvez pas formater les partitions en lecture seule.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir formater des partitions.

Avant de formater la partition, assurez-vous que :

- 1 La carte est activée.
- 1 La partition n'est pas connectée.
- 1 La carte n'est pas protégée contre l'écriture.
- 1 Une opération d'initialisation n'est pas déjà en cours sur la carte.

Pour formater la partition vFlash :

1. Sur l'interface Web iDRAC6, sélectionnez **Système**→ onglet **vFlash**→ sous-onglet **Formater**. La page **Formater** s'affiche.
2. Entrez les informations mentionnées dans [Tableau 11-4](#).
3. Cliquez sur **Appliquer**. Un message d'avertissement indiquant que toutes les données de la partition seront effacées s'affiche. Cliquez sur **OK**. La partition sélectionnée est formatée avec le type de système de fichiers spécifié.

Un message d'erreur apparaît si :

- 1 La carte est protégée contre l'écriture.
- 1 Une opération d'initialisation est déjà en cours sur la carte.

Tableau 11-4. Options de la page **Formater la partition**

Champ	Description
Nom	Sélectionnez le nom de la partition que vous voulez formater. La première partition disponible est sélectionnée par défaut. Toutes les partitions existantes du type Disquette ou Disque dur sont disponibles dans la liste déroulante. Les partitions qui sont connectées ou qui sont en lecture seule ne sont pas disponibles dans la liste déroulante.
Type de formatage	Sélectionnez le type de système de fichiers pour le formatage de la partition. Les options disponibles sont EXT2, EXT3, FAT16 et FAT32. Pour la carte SD standard, seul FAT32 est disponible.

Affichage des partitions disponibles

Vérifiez que la carte SD vFlash ou standard est activée pour pouvoir afficher la liste des partitions disponibles.

Pour afficher les partitions disponibles sur la carte :

1. Sur l'interface Web iDRAC6, sélectionnez **Système**→ **vFlash**→ sous-onglet **Gérer**. La page **Gérer les partitions** répertorie les partitions disponibles.
2. Pour chaque partition, vous pouvez afficher les informations mentionnées dans [Tableau 11-5](#).

Tableau 11-5. Affichage des partitions disponibles

Champ	Description
Index	Les partitions sont indexées de 1 à 16. L'index de partition est propre à une partition donnée. Il est spécifié lors de la création de la partition.
Nom	Identifie la partition. Il est spécifié lors de la création de la partition.
Taille	Taille de la partition en mégaoctets (Mo).
Lecture seule	État de l'accès en lecture-écriture de la partition. <ul style="list-style-type: none">1 Coché = partition en lecture seule.1 Décoché = partition en lecture-écriture. REMARQUE : Pour la carte SD standard, la partition est en lecture-écriture et cette colonne n'est pas affichée.

Connecté	Indique si la partition est visible au système d'exploitation en tant que périphérique USB. Pour connecter ou déconnecter des partitions, consultez la section Connexion et déconnexion d'une partition .
Type d'émulation	Indique si le type de partition est Disquette, Disque dur ou CD.
Type	Indique si le type de partition est Disquette, Disque dur ou CD.

Modification d'une partition

Vérifiez que la carte est activée pour pouvoir modifier la partition.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir modifier une partition vFlash.

Vous pouvez modifier une partition en lecture seule pour qu'elle devienne une partition en lecture-écriture ou vice-versa. Pour ce faire :

1. Sur l'interface Web iDRAC6, sélectionnez **Système** → onglet **vFlash** → sous-onglet **Gérer**. La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Lecture seule**, cochez la case correspondant aux partitions que vous voulez remplacer par des partitions en lecture seule ou décochez la case correspondant aux partitions que vous voulez remplacer par des partitions en lecture-écriture.

 **REMARQUE :** Si la partition est du type CD, l'état est en lecture seule et la case à cocher est sélectionnée. Vous ne pouvez pas remplacer l'état par l'état en lecture seule.
Si la partition est connectée, la case à cocher est grisée.
Pour la carte SD standard, la partition est en lecture-écriture et la colonne **Lecture seule** n'est pas affichée.

3. Cliquez sur **Appliquer**. Les partitions sont remplacées par des partitions en lecture seule ou en lecture-écriture selon vos sélections.

Connexion et déconnexion d'une partition

Vous pouvez connecter une ou plusieurs partitions en tant que périphériques de stockage de masse USB virtuels afin qu'ils soient visibles au système d'exploitation et au BIOS en tant que périphériques de stockage de masse. Lorsque plusieurs partitions sont connectées simultanément, elles sont présentées dans l'ordre ascendant au système d'exploitation hôte selon l'index. Les attributions correspondantes de lettre de lecteur sont contrôlées par le système d'exploitation.

Si vous déconnectez une partition, elle n'apparaît plus comme un périphérique de stockage de masse USB virtuel sur le système d'exploitation hôte et elle est supprimée du menu de la séquence d'amorçage du BIOS.

Si vous connectez ou déconnectez une partition, le bus USB du système est réinitialisé. Ceci peut affecter les applications (telles que le système d'exploitation) qui utilisent vFlash et mettra fin aux sessions de média virtuel d'iDRAC.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir connecter ou déconnecter une partition.

Avant de connecter ou de déconnecter une partition, assurez-vous que :

1. La carte est activée.
1. Une opération d'initialisation n'est pas déjà en cours sur la carte.

Pour connecter ou déconnecter des partitions :

1. Sur l'interface Web iDRAC6, sélectionnez **Système** → onglet **vFlash** → sous-onglet **Gérer**. La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Connecté**, cochez la case correspondant aux partitions que vous voulez connecter ou décochez la case correspondant aux partitions que vous voulez déconnecter.

 **REMARQUE :** Les partitions déconnectées ne sont pas affichées dans la séquence d'amorçage.

3. Cliquez sur **Appliquer**. Les partitions sont connectées ou déconnectées selon vos sélections.

Comportement du système d'exploitation en présence de partitions connectées

Lorsque les partitions sont connectées et que le système d'exploitation hôte est Windows, les lettres de lecteur qui sont attribuées aux partitions connectées sont contrôlées par le système d'exploitation.

Si une partition est en lecture seule, elle sera en lecture seule pour le système d'exploitation hôte.

Si le système d'exploitation hôte ne prend pas en charge le système de fichiers d'une partition connectée, vous ne pouvez pas lire ni modifier le contenu de la partition depuis le système d'exploitation hôte. Par exemple, le type de partition EXT2 ne peut pas être lu depuis le système d'exploitation Windows.

Lorsque vous modifiez le nom d'une partition connectée depuis le système d'exploitation hôte, cela n'affecte pas le nom stocké par iDRAC pour cette partition.

Suppression de partitions existantes

 **REMARQUE :** Vous pouvez supprimer des partitions existantes pour la carte SD vFlash ou standard.

Avant de supprimer des partitions existantes, assurez-vous que :

- 1 La carte n'est pas protégée contre l'écriture.
- 1 La partition n'est pas connectée.
- 1 Une opération d'initialisation n'est pas déjà en cours sur la carte.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir modifier une partition.

Pour supprimer une partition existante :

1. Sur l'interface Web iDRAC6, sélectionnez **Système**→onglet **vFlash**→ sous-onglet **Gérer**. La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Supprimer**, cliquez sur l'icône de suppression pour les partitions que vous voulez supprimer, puis cliquez sur **Appliquer**. Les partitions sont supprimées.

Téléchargement du contenu d'une partition

Vous pouvez télécharger le contenu d'une partition vFlash vers un emplacement local ou distant sous la forme d'un fichier image au format **.img** ou **.iso**. L'emplacement local se trouve sur votre système de gestion depuis lequel vous utilisez l'interface Web iDRAC6. L'emplacement distant se situe sur un système géré.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir télécharger des partitions.

Avant de télécharger le contenu vers un emplacement local ou distant, assurez-vous que :

- 1 La carte est activée.
- 1 Une opération d'initialisation n'est pas déjà en cours sur la carte.
- 1 Pour une partition en lecture-écriture, celle-ci ne doit pas être connectée.

Pour télécharger le contenu de la partition vFlash vers un emplacement de votre système :

1. Sur l'interface Web iDRAC6, sélectionnez **Système**→onglet **vFlash**→ sous-onglet **Télécharger**. La page **Télécharger une partition** s'affiche.
2. Dans le menu déroulant **Nom**, sélectionnez la partition que vous voulez télécharger. Toutes les partitions existantes sont affichées dans la liste, excepté les partitions qui sont connectées. La première partition est sélectionnée par défaut.
3. Cliquez sur **Télécharger**.
4. Spécifiez l'emplacement d'enregistrement du fichier.

Si seul l'emplacement du dossier est spécifié, le nom de la partition est alors utilisé comme nom de fichier, avec l'extension **.iso** pour les partitions de type CD et **.img** pour les partitions de type Disquette et Disque dur.
5. Cliquez sur **Enregistrer**. Le contenu de la partition sélectionnée est téléchargé vers l'emplacement spécifié.

Démarrage sur une partition

Vous pouvez définir une partition vFlash connectée comme périphérique de démarrage pour l'opération de démarrage suivante. La partition vFlash doit contenir une image d'amorçage (au format **.img** ou **.iso**) pour pouvoir la définir comme périphérique de démarrage. Vérifiez que la carte est activée pour pouvoir définir une partition comme périphérique de démarrage et pour pouvoir effectuer l'opération de démarrage.

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir définir une partition comme périphérique de démarrage.

Vous pouvez effectuer l'opération de démarrage pour la carte SD vFlash ou standard. Pour connaître les étapes à suivre, consultez la section [Périphérique de démarrage initial](#).

 **REMARQUE :** Si le BIOS du système ne prend pas en charge vFlash comme périphérique de démarrage initial, les partitions vFlash connectées risquent alors de ne pas figurer dans le menu déroulant **Périphérique de démarrage initial**. Veillez par conséquent à bien mettre le BIOS à jour vers la dernière version prenant en charge la configuration de la partition vFlash en tant que périphérique de démarrage initial. Si le BIOS comporte la dernière version, le redémarrage du serveur obligera le BIOS à informer iDRAC qu'il prend en charge vFlash comme périphérique de démarrage initial et iDRAC répertoriara la partition vFlash dans le menu déroulant **Périphérique de démarrage initial**.

Gestion des partitions vFlash à l'aide de la RACADM

Vous pouvez utiliser la sous-commande `vFlashPartition` pour créer, supprimer, répertorier ou afficher la condition des partitions sur une carte SD vFlash ou standard déjà initialisée. Le format est le suivant :

```
racadm vflashpartition <liste | condition | création | suppression> <options>
```

 **REMARQUE :** Vous devez disposer des privilèges Accès au média virtuel pour pouvoir gérer une partition vFlash.

Options valides :

<code>-i <index></code>	Index de la partition à laquelle s'applique cette commande. <code><index></code> doit être un entier compris entre 1 et 16. REMARQUE : Pour la carte SD standard, la valeur d'index est limitée à 1, car une seule partition de 256 Mo est prise en charge.
-------------------------------	---

Options valides uniquement pour l'action de création :

<code>-o <nom></code>	Nom affiché lors du montage de la partition sur le système d'exploitation. <code><nom></code> doit être une chaîne de six caractères alphanumériques maximum et ne doit pas contenir d'espaces.
<code>-e <type></code>	Type d'émulation de la partition. <code><type></code> doit être Disquette, CD-ROM ou Disque dur.
<code>-t <type></code>	Créez une partition du type <code><type></code> . <code><type></code> doit être : <ul style="list-style-type: none">1 vide : créez une partition vide.<ul style="list-style-type: none">o <code>-s <taille></code> : taille de la partition en Mo.o <code>-f <type></code> : type de format de la partition selon le type de système de fichiers. Les options valides sont RAW, FAT16, FAT32, EXT2 ou EXT3.1 image : créez une partition à l'aide d'un fichier image. Les options suivantes sont valides avec le type d'image :<ul style="list-style-type: none">o <code>-l <chemin></code> : spécifie le chemin distant par rapport à iDRAC. Le chemin peut se trouver sur un lecteur monté ou sur un partage : Chemin SMB : <code>//<ip ou domaine>/<nom_partage>/<chemin_vers_image></code> Chemin NFS : <code><adresseip>:/<chemin_vers_image></code>o <code>-u <utilisateur></code> : nom d'utilisateur permettant d'accéder à l'image distante. <code>-p <mot de passe></code> : mot de passe permettant d'accéder à l'image distante.

Options valides uniquement pour l'action de condition :

<code>-i</code>	Affiche la condition de l'index de partition.
-----------------	---

Création d'une partition

- 1 Pour créer une partition vide de 20 Mo :

```
racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20
```

- 1 Pour créer une partition à l'aide d'un fichier image situé sur un système distant :

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/foo.iso -u root -p mypassword
```

 **REMARQUE :** La création d'une partition à l'aide d'un fichier image n'est pas prise en charge dans la RACADM locale.

Suppression d'une partition

- 1 Pour supprimer une partition :

```
racadm vflashpartition delete -i 1
```

- 1 Pour supprimer toutes les partitions, réinitialisez la carte SD vFlash. Pour plus d'informations, consultez [Initialisation de la carte SD vFlash ou standard](#).

Obtention de la condition d'une partition

- 1 Pour obtenir la condition d'une opération sur la partition 1 :

```
racadm vflashpartition status -i 1
```

- 1 Pour obtenir la condition de toutes les partitions existantes :

```
racadm vflashpartition status -a
```

Affichage des informations des partitions

Pour énumérer toutes les partitions existantes et leurs propriétés :

```
racadm vflashpartition list
```

Démarrage sur une partition

- 1 Pour énumérer les périphériques disponibles dans la liste de démarrage :

```
racadm getconfig -g cfgServerInfo -o cfgServerFirstBootDevice
```

S'il s'agit d'une carte SD vFlash, les noms des partitions connectées apparaissent dans la liste de démarrage. S'il s'agit d'une carte SD standard et si la partition est connectée, VFLASH apparaît dans la liste de démarrage.

- 1 Pour définir une partition vFlash en tant que périphérique de démarrage :

```
racadm config -g cfgServerInfo -o cfgServerFirstBootDevice « <nom de la partition vFlash> »
```

où <nom de la partition vFlash> est le nom de la carte SD vFlash, ou VFLASH pour la carte SD standard.

Lorsque vous exécutez cette commande, le nom de la partition vFlash est automatiquement défini sur Démarrer une seule fois, c'est-à-dire que `cfgserverBootOnce` est défini sur 1. Démarrer une seule fois permet de démarrer le périphérique sur la partition une seule fois et ne le maintient pas constamment à la première place dans la séquence d'amorçage.

Connexion ou déconnexion d'une partition

- 1 Pour connecter une partition :

```
racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAttachState 1
```

- 1 Pour déconnecter une partition :

```
racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAttachState 0
```

Modification d'une partition

- 1 Pour modifier une partition en lecture seule pour qu'elle devienne une partition en lecture-écriture :

```
racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAccessType 1
```

- 1 Pour modifier une partition en lecture-écriture pour qu'elle devienne une partition en lecture seule :

```
racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAccessType 0
```

Pour plus d'informations sur les sous-commandes RACADM et sur les définitions des groupes et des objets de la base de données des propriétés d'iDRAC6, consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Questions les plus fréquentes

Quand la carte SD vFlash ou standard est-elle verrouillée ?

Le média flash virtuel est verrouillé par iDRAC lorsque l'opération qu'il effectue requiert un accès exclusif au média. Par exemple, au cours d'une opération d'initialisation.

[Retour à la page du sommaire](#)

Configuration et utilisation du média virtuel

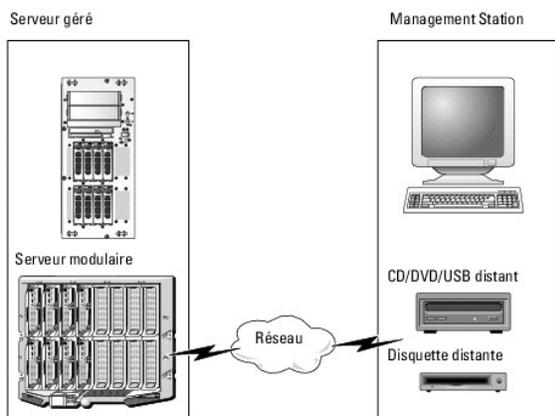
Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Présentation](#)
- [Configuration du média virtuel](#)
- [Exécution du média virtuel](#)
- [Questions les plus fréquentes](#)

Présentation

La fonctionnalité Média virtuel, accessible via le visualiseur de console virtuelle, permet au serveur géré d'accéder au média connecté à un système distant sur le réseau. [Figure 12-1](#) illustre l'architecture globale d'un média virtuel.

Figure 12-1. Architecture globale d'un média virtuel



Grâce au média virtuel, les administrateurs peuvent démarrer à distance leurs serveurs gérés, installer des applications, mettre à jour des pilotes ou même installer de nouveaux systèmes d'exploitation à distance à partir de lecteurs de CD/DVD et de disquettes virtuels.

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

Le média virtuel définit deux périphériques pour le système d'exploitation et le BIOS du serveur géré : un périphérique de disquette et un périphérique de disque optique.

La station de gestion fournit le média physique ou le fichier image sur le réseau. Lorsque le média virtuel est connecté, toutes les requêtes d'accès au lecteur de CD ou de disquette virtuel provenant du serveur géré sont dirigées vers la station de gestion par le biais du réseau. La connexion du média virtuel est identique à l'insertion du média dans des périphériques physiques sur le système géré. Lorsque le média virtuel se trouve en 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.

[Tableau 12-1](#) 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 12-1. Connexions de lecteur prises en charge

Connexions de lecteur de disquette virtuel prises en charge	Connexions de lecteur optique virtuel prises en charge
Lecteur de disquette 1.44 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 USB amovible (taille minimale 128 Mo)	

Station de gestion Windows

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

Selon votre version d'Internet Explorer, vous devrez peut-être définir un paramètre de sécurité personnalisé pour ActiveX :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils**→ **Options Internet**, puis sur l'onglet **Sécurité**.
3. Sous **Sélectionnez une zone de contenu Web pour spécifier ses paramètres de sécurité**, cliquez pour sélectionner la zone souhaitée.
4. Sous **Niveau de sécurité pour cette zone**, cliquez sur **Personnaliser le niveau**.
La fenêtre **Paramètres de sécurité** s'affiche.
5. Sous **Contrôles ActiveX et plug-ins**, vérifiez que les paramètres suivants sont définis sur **Activé** :
 - 1 Autoriser les scriptlets
 - 1 Demander confirmation pour les contrôles ActiveX
 - 1 Télécharger les contrôles ActiveX signés
 - 1 Télécharger les contrôles ActiveX non signés
6. Cliquez sur **OK** pour enregistrer les modifications et fermer la fenêtre **Paramètres de sécurité**.
7. Cliquez sur **OK** pour fermer la fenêtre **Options Internet**.
8. Redémarrez Internet Explorer.

Vous devez disposer de droits d'administrateur pour installer ActiveX. Avant d'installer le contrôle ActiveX, Internet Explorer peut afficher un avertissement de sécurité. Pour terminer la procédure d'installation du contrôle ActiveX, acceptez le contrôle ActiveX lorsqu'Internet Explorer affiche un avertissement de sécurité.

Station de gestion Linux

Pour exécuter la fonctionnalité 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) est requis pour exécuter le plug-in de console virtuelle. Vous pouvez télécharger un JRE à l'adresse java.sun.com.

Configuration du média virtuel

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur **Système**→ **Console virtuelle/Média virtuel**→ **Configuration**.
3. Dans la section Média virtuel, sélectionnez des valeurs de paramètres. Consultez la section [Tableau 12-2](#) pour plus d'informations sur les valeurs de configuration du média virtuel.
4. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Le message d'alerte suivant s'affiche : You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue? (Vous êtes sur le point de modifier la configuration du périphérique. Toutes les sessions de redirection existantes seront fermées. Voulez-vous continuer ?)

5. Cliquez sur **OK** pour continuer.

Le message d'alerte suivant s'affiche : Virtual Media Configuration successfully set. (Configuration du média virtuel terminée).

Tableau 12-2. Valeurs de configuration du média virtuel

Attribut	Valeur
Connecter le média virtuel	Connecter : connecte immédiatement le média virtuel au serveur. Déconnecter : déconnecte immédiatement le média virtuel du serveur. Autoconnecter : connecte le média virtuel au serveur uniquement lorsqu'une session de média virtuel est démarrée.
Nombre maximal de sessions	Affiche le nombre maximal de sessions de média virtuel autorisé. Ce nombre est toujours 1.

	REMARQUE : Une seule session utilisateur du média virtuel est autorisée, mais plusieurs périphériques peuvent être connectés au cours d'une même session. Consultez Exécution du média virtuel .
Sessions actives	Affiche le nombre de sessions de média virtuel actuellement actives.
Cryptage de média virtuel activé	Active (coché) ou désactive (non coché) le cryptage sur les connexions de média virtuel.
Émulation de disquette	Indique si le média virtuel apparaît au serveur comme un lecteur de disquette ou une clé USB. Si Émulation de disquette est sélectionné, le périphérique de média virtuel apparaît comme un périphérique de disquette sur le serveur. Si elle désélectionnée, il apparaît comme un lecteur de clé USB. REMARQUE : Dans certains environnements Windows Vista et Red Hat Enterprise Linux, il est possible que vous ne puissiez pas virtualiser un périphérique USB avec Émulation de disquette activé.
Activer le démarrage unique	Active (coché) ou désactive (non coché) l'option Démarrer une seule fois qui termine automatiquement la session du média virtuel après le premier démarrage du serveur. 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 est utile pour les déploiements automatisés.

Exécution du média virtuel

 **PRÉCAUTIONS :** N'émettez pas de 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 virtuelle doit rester active pendant que vous accédez au média virtuel.

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Cliquez sur l'onglet **Console virtuelle/Média virtuel**.

L'écran **Console virtuelle et média virtuel** s'affiche.

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

4. Cliquez sur **Lancer la console virtuelle**.

 **REMARQUE :** Sous Linux, le fichier `jviewer.jnlp` est téléchargé sur votre bureau et une boîte de dialogue vous demande ce que vous souhaitez faire avec le fichier. Choisissez l'option **Ouvrir avec le programme**, puis sélectionnez l'application `javaws` qui se trouve dans le sous-répertoire `bin` de votre répertoire d'installation JRE.

L'application **iDRACView** se lance dans une fenêtre distincte.

5. Sélectionnez **Média** → **Assistant Média virtuel**.

La fenêtre **Redirection de média** apparaît.

6. Affichez la section **Condition** au bas de la fenêtre **Redirection de média**. Si le média est connecté, vous pouvez le déconnecter avant d'établir une connexion avec une source de média différente. Pour déconnecter un média, cliquez sur le bouton **Déconnecter** situé en regard du média dans la fenêtre **Condition**.
7. Sélectionnez le bouton radio situé en regard des types de média que vous souhaitez connecter.
8. Vous pouvez sélectionner le bouton radio **Image disquette** et un autre dans la section **Lecteur de CD/DVD**.

 **REMARQUE :** Lorsque le média CD/DVD d'une station de gestion est déjà utilisé par le serveur lame iDRAC6, ce même média peut être redirigé et mis à la disposition d'une autre serveur lame iDRAC6. En d'autres termes, iDRAC6 prend en charge la redirection du même média (lecture seule) vers deux serveurs lames iDRAC6 différents. Dans le cas d'un média USB, vous ne pourrez toutefois pas vous connecter à deux serveurs lames iDRAC6. iDRAC6 affiche un message d'avertissement l'indiquant également.

Si vous souhaitez connecter une image de disquette ou une image ISO, entrez le chemin d'accès à l'image sur votre ordinateur local ou cliquez sur le bouton **Parcourir** et recherchez l'image.

 **REMARQUE :** Si vous utilisez le plug-in Java du média virtuel, il se peut que vous ne puissiez pas monter des images ISO distantes. Par exemple, les clients Linux ne vous permettront pas de monter des images car ils utilisent le plug-in Java. Pour éviter ce problème, copiez l'image ISO sur votre système local afin que le fichier image soit disponible localement. Le plug-in Java du média virtuel ne vous permet pas de spécifier le nom de partage au format \\computer\share.

9. Cliquez sur le bouton **Connecter** **situé en regard de chaque type de média sélectionné.**

Le média est connecté et la fenêtre **Condition** est mise à jour.

10. Cliquez sur **Fermer.**

 **REMARQUE :** À chaque fois qu'une session de média virtuel est lancée ou qu'un disque vFlash est connecté, un lecteur supplémentaire nommé « 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.

Déconnexion du média virtuel

1. Sélectionnez **Média** → **Assistant Média virtuel.**

L'**Assistant Redirection de média** apparaît.

2. Cliquez sur le bouton **Déconnecter** situé en regard du média que vous souhaitez déconnecter.

Le média est déconnecté et la fenêtre **Condition** est mise à jour.

3. Cliquez sur **Fermer.**

 **REMARQUE :** Lorsque vous lancez **iDRACview** puis fermez votre session de l'interface utilisateur Web, **iDRACView** ne se ferme pas et demeure actif.

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, suivez 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 d'amorçage. Si nécessaire, suivez les instructions affichées à l'écran pour modifier la séquence d'amorçage.
5. Enregistrez les modifications et quittez.

Le serveur géré redémarre.

Le serveur géré tente de démarrer à partir d'un périphérique d'amorçage en suivant la séquence d'amorçage. Si le périphérique virtuel est connecté et qu'un média d'amorçage est présent, le système démarre sur le périphérique virtuel. Autrement, le système ignore le périphérique, tout comme un périphérique physique sans média d'amorçage.

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 sous forme de script du système d'exploitation utilisant le média virtuel peut prendre moins de 15 minutes. Consultez la section [Déploiement du système d'exploitation](#) pour plus d'informations.

1. Vérifiez les points suivants :

- 1 Le DVD/CD d'installation de votre système d'exploitation est inséré dans le lecteur de DVD/CD de la station de gestion.
- 1 Le lecteur de DVD/CD local est sélectionné.
- 1 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 vous assurer que le BIOS est

configuré pour démarrer à partir du lecteur de DVD/CD à partir duquel vous effectuez l'installation.

3. Suivez les instructions à l'écran pour terminer l'installation.

Utilisation d'un média virtuel 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 ne peuvent pas être montés automatiquement. Si vos lecteurs ne sont pas montés automatiquement, montez-les manuellement à l'aide de la commande **mount** Linux.

Questions les plus fréquentes

[Tableau 12-3](#) répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 12-3. Utilisation d'un média virtuel : Questions les plus fréquentes

Question	Réponse
Je remarque parfois que ma connexion client au Média virtuel est interrompue. Pourquoi ?	<p>Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel.</p> <p>Si les paramètres de configuration du média virtuel sont modifiés dans l'interface Web iDRAC6 ou via les commandes RACADM locales, tout média connecté est déconnecté lorsque les modifications de la configuration sont appliquées.</p> <p>Pour rétablir la connexion au lecteur virtuel, utilisez l'Assistant Média virtuel.</p>
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 pris en charge par iDRAC6 ?	Pour obtenir 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 ?	<ol style="list-style-type: none">1 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'interface utilisateur et continuez l'opération précédente.1 Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. En outre, il se peut que quelqu'un ait modifié les paramètres de configuration du média virtuel dans l'interface Web ou en ayant entré des commandes RADACM. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité Média virtuel.
Une installation du système d'exploitation Windows semble prendre trop longtemps. Pourquoi ?	Si vous installez le système d'exploitation Windows et que votre 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.
Je visualise le contenu d'un lecteur de disquette ou d'une clé mémoire USB. Si j'essaie d'établir une connexion au média virtuel en utilisant le même lecteur, je reçois un message d'échec de connexion et le système me demande de réessayer. Pourquoi ?	L'accès simultané aux lecteurs de disquette virtuels n'est pas autorisé. Fermez l'application utilisée pour visualiser le contenu du lecteur avant d'essayer de virtualiser le lecteur.
Comment puis-je configurer mon périphérique virtuel comme périphérique d'amorçage ?	Sur le serveur géré, accédez à la configuration du BIOS, puis au menu de démarrage. Recherchez le CD virtuel, la disquette virtuelle ou le disque Flash virtuel et changez la séquence d'amorçage des périphériques, si nécessaire. Par exemple, pour démarrer à partir d'un lecteur de CD, définissez-le en tant que premier lecteur dans la séquence d'amorçage.
À partir de quels types de média puis-je démarrer ?	iDRAC6 vous permet de démarrer à partir des médias d'amorçage suivants : <ul style="list-style-type: none">1 Média de données de CD-ROM/DVD1 Image ISO 96601 Disquette 1.44 ou image de disquette1 Clé USB reconnue par le système d'exploitation comme disque amovible (taille minimale 128 Mo)1 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.

	<p>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, entrez la commande suivante :</p> <pre>sys a: x: /s</pre> <p>où x: est la clé USB que vous voulez utiliser comme clé de démarrage.</p>
<p>Quels types de systèmes de fichiers sont pris en charge sur mon lecteur de disquette virtuel ?</p>	<p>Votre lecteur de disquette virtuel prend en charge les systèmes de fichiers FAT16 ou FAT32.</p>
<p>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 ?</p>	<p>Les mises à jour de micrologiciel entraînent une réinitialisation d'iDRAC6, une interruption de la connexion à distance et le démontage des lecteurs virtuels. Les lecteurs réapparaîtront une fois la réinitialisation d'iDRAC6 terminée.</p>
<p>Je n'arrive pas à trouver mon lecteur de disquette 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 ?</p>	<p>Certaines versions de Linux ne montent pas automatiquement le lecteur de disquette virtuel et le lecteur de CD virtuel de la même manière. Pour installer le lecteur de disquette virtuel, recherchez le nud de périphérique que Linux attribue au lecteur de disquette virtuel. Suivez les étapes suivantes pour rechercher et monter correctement le lecteur de disquette virtuel :</p> <ol style="list-style-type: none"> 1. Ouvrez une invite de commande Linux et exécutez la commande suivante : <pre>grep "Virtual Floppy" /var/log/messages</pre> 2. Recherchez la dernière entrée de ce message et notez l'heure. 3. À l'invite de Linux, exécutez la commande suivante : <pre>grep "hh:mm:ss" /var/log/messages</pre> <p>où :</p> <pre>hh:mm:ss</pre> <p>correspond à l'horodatage du message renvoyé par grep à l'étape 1.</p> 4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique attribué à la disquette virtuelle Dell. 5. Assurez-vous que vous êtes relié et connecté au lecteur de disquette virtuel. 6. À l'invite de Linux, exécutez la commande suivante : <pre>mount /dev/sdx /mnt/floppy</pre> <p>où :</p> <pre>/dev/sdx</pre> <p>est le nom du périphérique trouvé à l'étape 4</p> <pre>/mnt/floppy</pre> <p>est le point de montage.</p>

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation de l'interface de ligne de commande RACADM

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Sous-commandes RACADM](#)
- [Utilisation de commandes RACADM locales](#)
- [Utilisation de l'utilitaire RACADM pour configurer iDRAC6](#)
- [RACADM distante et SSH/Telnet](#)
- [Utilisation d'un fichier de configuration iDRAC6](#)
- [Configuration de plusieurs iDRAC6](#)

L'interface de ligne de commande (CLI) RACADM permet d'accéder aux fonctionnalités de gestion iDRAC6 du serveur géré. La RACADM permet d'accéder à la plupart des fonctionnalités de l'interface Web iDRAC6. La RACADM peut être utilisée dans les scripts afin de faciliter la configuration de plusieurs serveurs, au lieu d'utiliser l'interface Web, qui convient davantage à la gestion interactive.

Les interfaces suivantes sont disponibles pour la RACADM :

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

Les commandes RACADM locales n'utilisent pas les connexions réseau pour accéder à iDRAC6 à partir du serveur géré. Cela signifie que vous pouvez utiliser les commandes RACADM locales pour configurer la mise en réseau iDRAC6 initiale. RACADM distante est un utilitaire côté client, qui peut être exécuté à partir d'une station de gestion via l'interface réseau hors bande. RACADM SSH/Telnet est utilisée pour faire référence à l'utilisation de la commande RACADM à partir de l'invite SSH ou Telnet.

Cette section fournit les informations suivantes :

- 1 Les commandes RACADM et les interfaces RACADM prises en charge
- 1 Utilisation de la RACADM locale à partir d'une invite de commande
- 1 RACADM distante
- 1 RACADM SSH/Telnet
- 1 Configuration de votre iDRAC6 à l'aide de la commande `racadm`
- 1 Utilisation du fichier de configuration RACADM pour configurer plusieurs iDRAC6

⚠ PRÉCAUTIONS : Le dernier micrologiciel iDRAC6 prend uniquement en charge la dernière version de la RACADM. Vous pouvez rencontrer des erreurs si vous utilisez une version plus ancienne de la RACADM pour interroger un iDRAC6 doté du dernier micrologiciel. Installez la version de la RACADM fournie avec votre dernier DVD Dell OpenManage.

Sous-commandes RACADM

Tableau 13-1 fournit une description de chaque sous-commande RACADM que vous pouvez exécuter dans la RACADM. Pour une liste détaillée des sous-commandes RACADM incluant la syntaxe et les entrées valides, consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Tableau 13-1. Sous-commandes RACADM

Commande	Description
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 (ASR).
closessn	Ferme une session de communication sur le périphérique.
coredump	Affiche la dernière image mémoire iDRAC6.
coredumpdelete	Supprime l'image mémoire stockée sur l'iDRAC6.
clrraclog	Efface le journal iDRAC6. Une fois cette opération effectuée, une entrée unique est effectuée pour indiquer l'utilisateur et l'heure à laquelle le journal a été effacé.
clrsel	Efface les entrées du journal des événements système du serveur géré.
config	Configure iDRAC6.
fwupdate	Met à jour le micrologiciel iDRAC6.
getconfig	Affiche les propriétés de configuration iDRAC6 actuelles.
getniccfg	Affiche la configuration IP actuelle du contrôleur.
getraclog	Affiche le journal iDRAC6.
getractime	Affiche l'heure iDRAC6.
getsel	Affiche les entrées du journal SEL.
getssninfo ¹	Affiche des informations sur les sessions actives.

getsvctag	Affiche le numéro de service.
getsysinfo	Affiche des informations sur iDRAC6 et le serveur géré, y compris des informations sur la configuration IP, le modèle de matériel, les versions du micrologiciel et sur le système d'exploitation.
gettracelog	Affiche le journal de suivi d'iDRAC6. Si elle est utilisée avec -i, la commande affiche le nombre d'entrées du journal de suivi iDRAC6.
help	Répertorie les sous-commandes iDRAC6.
help < sous-commande >	Répertorie les instructions d'utilisation pour la sous-commande spécifiée.
ifconfig	Affiche le contenu de la table d'interface réseau.
krbkeytabupload	Téléverse le fichier keytab Kerberos.
localconredirdisable	Effectue la désactivation de la console virtuelle locale à partir du système local.
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. Une adresse IP de destination est requise. Un paquet d'écho ICMP est envoyé à l'adresse IP de destination en fonction du contenu actuel de la table de routage.
ping6	Vérifie que l'adresse IPv6 de destination est accessible à partir d'iDRAC6 avec le contenu actuel de la table de routage. Une adresse IPv6 de destination est requise. Un paquet d'écho ICMP est envoyé à l'adresse IPv6 de destination en fonction du contenu actuel de la table de routage.
racdump	Affiche des informations sur la condition et des informations générales concernant iDRAC6.
racreset	Réinitialise iDRAC6.
racresetcfg	Restaure la configuration par défaut iDRAC6.
remotefimage	Partage de fichiers distants
serveraction	Effectue des opérations de gestion de l'alimentation sur le serveur géré.
setniccfg	Définit la configuration IP du contrôleur.
sshpkeyauth	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.
sslcertdownload	Télécharge un certificat d'AC.
sslcertupload	Téléverse un certificat d'autorité de certification ou un certificat de serveur sur iDRAC6.
sslcertview	Affiche un certificat d'autorité de certification ou un certificat de serveur iDRAC6.
sslcsrgen	Génère et télécharge la RSC SSL.
testemail	Force iDRAC6 à envoyer un e-mail en passant par le NIC iDRAC6.
testtrap	Force iDRAC6 à envoyer une alerte SNMP en passant par le NIC iDRAC6.
traceroute	Effectue le suivi du chemin réseau de routeurs que les paquets empruntent lorsqu'ils sont transférés de votre système vers une adresse IPv4 de destination.
traceroute6	Effectue le suivi du chemin réseau de routeurs que les paquets empruntent lorsqu'ils sont transférés de votre système vers une adresse IPv6 de destination.
version	Affiche les informations sur la version iDRAC6.
vflashsd	Initialise ou obtient la condition de la carte SD vFlash.
vflashpartition	Crée, supprime, répertorie ou affiche la condition des partitions d'une carte SD vFlash initialisée.
vmdisconnect	Ferme toutes les connexions du média virtuel iDRAC6 ouvertes à partir des clients distants.
vmkey	Réinitialise la taille par défaut de 256 Mo de la partition vFlash et supprime toutes les données de la partition.
¹ Les informations de la session SOL ne sont pas incluses dans la réponse à la commande getssninfo.	

Utilisation de commandes RACADM locales

Vous exécutez les commandes RACADM localement (sur le serveur géré) à partir d'une invite de commande ou d'une invite d'environnement.

Connectez-vous au serveur géré, démarrez un environnement de commande et entrez les commandes RACADM locales dans un des formats suivants :

```
1 racadm < sous-commande > [paramètres]
1 racadm <getconfig|config> [-g <groupe>] [-o <objet> <valeur>]
```

Sans options, la commande RACADM affiche des informations d'utilisation d'ordre général. Pour afficher la liste des sous-commandes RACADM, tapez :

```
racadm help
```

ou

```
racadm getconfig -h
```

La liste des sous-commandes inclut toutes les commandes RACADM prises en charge par iDRAC6.

Pour obtenir de l'aide concernant une sous-commande, tapez :

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

La commande affiche la syntaxe et les options de ligne de commande de la sous-commande.

Utilisation de l'utilitaire RACADM pour configurer iDRAC6

Cette section décrit comment utiliser la RACADM pour effectuer diverses tâches de configuration iDRAC6.

Affichage des paramètres iDRAC6 actuels

La sous-commande **getconfig** RACADM récupère les paramètres de configuration actuels à partir d'iDRAC6. Les valeurs de configuration sont organisées en *groupes* contenant un ou plusieurs *objets* ayant des *valeurs*.

Consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals pour une description complète des groupes et des objets.

Pour afficher la liste de tous les groupes iDRAC6, entrez la commande suivante :

```
racadm getconfig -h
```

Pour afficher les objets et les valeurs d'un groupe spécifique, entrez la commande suivante :

```
racadm getconfig -g <groupe>
```

Par exemple, pour afficher la liste de tous les paramètres d'objet du groupe **cfgLanNetworking**, entrez la commande suivante :

```
racadm getconfig -g cfgLanNetworking
```

Gestion des utilisateurs iDRAC6 avec la RACADM

 **REMARQUE :** Soyez prudent lorsque vous utilisez la commande **racresetcfg**, car les valeurs d'origine de *tous* les paramètres de configuration sont restaurées. Toute modification précédente est perdue.

 **REMARQUE :** 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**.

 **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.

 **REMARQUE :** Les utilisateurs et les groupes créés pour les environnements Active Directory doivent se conformer à la convention d'attribution de nom d'Active Directory.

Vous pouvez configurer jusqu'à 15 utilisateurs dans la base de données de propriétés iDRAC6. (Un seizième utilisateur est réservé pour l'utilisateur du LAN IPMI). Avant d'activer manuellement un utilisateur iDRAC6, vérifiez si des utilisateurs existent déjà.

Pour déterminer si un utilisateur existe, tapez la commande suivante à l'invite de commande :

```
racadm getconfig -u <nom d'utilisateur>
```

OU

tapez la commande suivante une fois pour tous les index de 1 à 16 :

```
racadm getconfig -g cfgUserAdmin -i <index>
```

 **REMARQUE :** Vous pouvez également taper **racadm getconfig -f <nom de fichier>** et afficher le fichier *<nom de fichier>* généré, qui inclut tous les utilisateurs, ainsi que tous les autres paramètres de configuration iDRAC6.

Plusieurs paramètres et références d'objet sont affichés avec leurs valeurs actuelles. Les deux objets d'intérêt sont :

```
# cfgUserAdminIndex=nn
```

```
cfgUserAdminUserName=
```

Si l'objet **cfgUserAdminUserName** n'a pas de valeur, ce numéro d'index, indiqué par l'objet **cfgUserAdminIndex**, peut être utilisé. S'il y a un nom après le signe **=**, cet index est attribué à ce nom d'utilisateur.

 **REMARQUE :** Les utilisateurs et les groupes créés pour les environnements Active Directory doivent se conformer à la convention d'attribution de nom d'Active Directory.

Ajout d'un utilisateur iDRAC6

Pour ajouter un nouvel utilisateur à iDRAC6, suivez les étapes suivantes :

1. Définissez le nom d'utilisateur.
2. Définissez le mot de passe.
3. Définissez l'ouverture de session sur les privilèges utilisateur iDRAC6.

4. Activez l'utilisateur.

Exemple

L'exemple suivant décrit comment ajouter un nouvel utilisateur appelé « Jean » avec un mot de passe « 123456 » et des privilèges d'ouverture de session iDRAC6 :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x00000001
racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

Pour vérifier le nouvel utilisateur, utilisez l'une des commandes suivantes :

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

Activation d'un utilisateur iDRAC6 avec des droits

Pour octroyer à un utilisateur des droits d'administration spécifiques (basés sur les rôles), définissez la propriété `cfgUserAdminPrivilege` sur un masque binaire construit à partir des valeurs affichées dans [Tableau 13-2](#) :

Tableau 13-2. Masques binaires pour les privilèges utilisateur

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

Par exemple, pour octroyer à l'utilisateur les privilèges **Configurer iDRAC6**, **Configurer les utilisateurs**, **Effacer les journaux** et **Accéder à la console virtuelle**, ajoutez les valeurs 0x00000002, 0x00000004, 0x00000008 et 0x00000010 pour construire le bitmap 0x0000002E. Ensuite, entrez la commande suivante pour définir le privilège :

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

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.

À partir d'une commande RACADM locale :

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

À partir de RACADM telnet/ssh :

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

Exemple :

Téléversez une clé valide vers l'utilisateur 2 iDRAC6 dans le premier espace de 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.

 **PRÉCAUTIONS :** 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
```

 **PRÉCAUTIONS :** Ce privilège est normalement réservé aux utilisateurs qui sont membres du groupe d'utilisateurs Administrateur sur iDRAC. Les utilisateurs du groupe d'utilisateurs « Personnalisé » peuvent toutefois bénéficier de ce privilège. Un utilisateur possédant ce privilège peut modifier la configuration de n'importe quel utilisateur. Ceci inclut la création ou la suppression de n'importe quel utilisateur, la gestion des clés SSH pour les utilisateurs, etc. Pour ces raisons, vous devez attribuer ce privilège avec prudence.

Consultez sshpkauth dans la *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals pour des informations sur les options des sous-commandes.

Suppression d'un utilisateur iDRAC6

Lorsque vous utilisez la RACADM, l'utilisateur iDRAC ne peut pas être supprimé. L'utilisateur peut uniquement être désactivé à l'aide de l'objet `cfgUserAdminEnable`. La syntaxe de commande est la suivante :

```
racadm config -g cfgUserAdmin -o cfgUserAdminEnable -I <index>
```

Pour plus d'informations sur la gestion des droits d'administration utilisateur, consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Test des alertes par e-mail

La fonctionnalité des alertes par e-mail iDRAC6 permet aux utilisateurs de recevoir des alertes par e-mail lorsqu'un événement critique se produit sur le serveur géré. L'exemple suivant montre comment tester la fonctionnalité des alertes par e-mail pour s'assurer qu'iDRAC6 peut correctement envoyer des alertes par e-mail sur le réseau.

```
racadm testemail -i 2
```

(-i 2 est pour l'entrée d'index n°2 dans le tableau d'alertes par e-mail)

 **REMARQUE :** Assurez-vous que les paramètres des alertes SMTP et par e-mail sont configurés avant de tester la fonctionnalité des alertes par e-mail. Consultez la section [Configuration des alertes par e-mail](#) pour plus d'informations.

Test de la fonctionnalité d'alertes par interruption SNMP iDRAC6

La fonctionnalité d'alertes par interruption SNMP iDRAC6 permet aux configurations d'écoute d'interruptions SNMP de recevoir des interruptions pour les événements système qui se produisent sur le serveur géré.

L'exemple suivant montre comment un utilisateur peut tester la fonctionnalité d'alertes par interruption SNMP.

```
racadm testtrap -i 2
```

(-i 2 est pour l'entrée d'index n°2 dans le tableau d'alertes par e-mail)

 **REMARQUE :** Avant de tester la fonctionnalité d'alertes par interruption SNMP d'iDRAC6, 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. Consultez la section [Configuration des interruptions d'événement sur plateforme \(PET\)](#) pour plus d'informations.

Configuration des propriétés réseau iDRAC6

Pour générer une liste des propriétés réseau disponibles, entrez la commande suivante :

```
racadm getconfig -g cfgLanNetworking
```

Pour utiliser DHCP pour obtenir une adresse IP, utilisez la commande suivante pour écrire l'objet `cfgNicUseDhcp` et activer cette fonctionnalité :

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

Les commandes fournissent la même fonctionnalité de configuration que l'utilitaire de configuration iDRAC6 lorsque vous êtes invité à appuyer sur <Ctrl><E>. Pour plus d'informations sur la configuration des propriétés réseau à l'aide de l'utilitaire de configuration d'iDRAC6, consultez [LAN iDRAC6](#).

L'exemple suivant montre comment la commande peut être utilisée pour configurer les propriétés réseau du LAN souhaitées.

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

 **REMARQUE :** Si la commande `cfgNicEnable` est définie sur 0, le LAN iDRAC6 est désactivé même si DHCP est activé.

Configuration d'IPMI sur le LAN

1. Configurez IPMI sur le LAN en entrant la commande suivante :

```
racadm config -g cfgIpmlan -o cfgIpmlanEnable 1
```

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

- a. Mettez à jour les privilèges de canal IPMI en entrant la commande suivante :

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

où <niveau> correspond à :

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

Par exemple, pour définir le privilège du canal LAN IPMI sur 2 (utilisateur), entrez la commande suivante :

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

- b. Définissez la clé de cryptage du canal LAN IPMI, le cas échéant, à l'aide d'une commande similaire à la suivante :

```
racadm config -g cfgIpmlan -o cfgIpmlanEncryptionKey <clé>
```

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

2. Configurez les communications série sur le LAN (SOL) IPMI à l'aide de la commande suivante :

```
racadm config -g cfgIpmlanSol -o cfgIpmlanSolEnable 1
```

 **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.

- a. Mettez à jour le niveau de privilège minimum SOL IPMI à l'aide de la commande suivante :

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

où <niveau> correspond à :

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

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

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

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

- b. Mettez à jour le débit en bauds SOL IPMI à l'aide de la commande suivante :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <débit en bauds>
```

où <débit en bauds> est égal à 19200, 57600 ou 115200 bits/s.

Par exemple :

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

- c. Activez les communications série sur le LAN en tapant la commande suivante à l'invite de commande.

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

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable 1 -i <référence>
```

où <référence> est la référence unique de l'utilisateur.

Configuration de PEF

Vous pouvez configurer l'action qu'iDRAC6 devra effectuer pour chaque alerte sur plateforme. [Tableau 13-3](#) répertorie les actions possibles et la valeur permettant de les identifier dans la RACADM.

Tableau 13-3. Action d'événement sur plateforme

Action	Valeur
Pas d'action	0
Hors tension	1
Redémarrer	2
Cycle d'alimentation	3

Configurez les actions PEF à l'aide de la commande suivante :

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <index> <valeur d'action>
```

où <index> est l'index PEF ([Tableau 5-8](#)) et <valeur d'action> est une valeur de [Tableau 13-3](#).

Par exemple, pour activer PEF pour redémarrer le système et envoyer une alerte IPMI lorsqu'un événement critique de processeur est détecté, entrez la commande suivante :

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
```

Configuration du PET

1. Activez les alertes globales à l'aide de la commande suivante :

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

2. Activez PET à l'aide de la commande suivante :

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <index> <0|1>
```

où <index> est l'index de destination PET et 0 ou 1 permet, respectivement, de désactiver PET ou d'activer PET.

Par exemple, pour activer le PET avec l'index 4, entrez la commande suivante :

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

3. Configurez votre règle PET à l'aide de la commande suivante :

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <index> <adresse IP>
```

où <index> est l'index de destination PET et <adresse IP> l'adresse IP de destination du système qui reçoit les alertes d'événement sur plateforme.

4. Configurez la chaîne Nom de communauté.

À l'invite de commande, entrez :

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

où <nom> est le nom de communauté PET.

Configuration des alertes par e-mail

1. Activez les alertes globales en entrant la commande suivante :

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

2. Activez les alertes par e-mail en entrant les commandes suivantes :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <index> <0|1>
```

où <index> est l'index de destination d'e-mail et 0 désactive l'alerte par e-mail ou 1 active l'alerte. L'index de destination d'e-mail peut être une valeur de 1 à 4.

Par exemple, pour activer l'e-mail avec l'index 4, entrez la commande suivante :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

3. Configurez vos paramètres de messagerie en entrant la commande suivante :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <adresse e-mail>
```

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

4. Pour configurer le serveur de messagerie SMTP, entrez la commande suivante :

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <Adresse IP?du serveur de messagerie SMTP>
```

5. Pour configurer un message personnalisé, entrez la commande suivante :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <index> <message personnalisé>
```

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

6. Testez l'alerte par e-mail configurée, si vous le souhaitez, en entrant la commande suivante :

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

où <index> est l'index de destination d'e-mail à tester.

Configuration du filtrage IP (plage IP)

Le filtrage des adresses IP (ou *contrôle de plage IP*) permet uniquement un accès à iDRAC6 à partir des clients ou stations de gestion dont les adresses IP sont comprises dans une plage spécifique à l'utilisateur. Toutes les autres requêtes d'ouverture de session sont rejetées.

Le filtrage IP compare l'adresse IP d'une ouverture de session entrante à la plage d'adresses IP qui est spécifiée dans les propriétés **cfgRacTuning** suivantes :

```
1 cfgRacTuneIpRangeAddr
1 cfgRacTuneIpRangeMask
```

La propriété **cfgRacTuneIpRangeMask** est appliquée à la fois à l'adresse IP entrante et aux propriétés **cfgRacTuneIpRangeAddr**. Si les résultats sont identiques, la requête d'ouverture de session entrante est autorisée pour pouvoir accéder à iDRAC6. Les ouvertures de session à partir d'adresses IP situées hors de cette plage reçoivent un message d'erreur.

L'ouverture de session a lieu si l'expression suivante est égale à zéro :

```
cfgRacTuneIpRangeMask & (<adresse IP entrante> ^ cfgRacTuneIpRangeAddr)
```

où & est l'opérateur de bits AND des quantités et ^ est l'opérateur de bits OR exclusif.

Consultez **cfgRacTuning** dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals pour une liste complète des propriétés **cfgRacTuning**.

Tableau 13-4. Propriétés de filtrage des adresses IP (Plage IP)

Propriété	Description
<code>cfgRacTuneIpRangeEnable</code>	Active la fonctionnalité Contrôle de plage IP.
<code>cfgRacTuneIpRangeAddr</code>	Détermine le format binaire d'adresse IP accepté en fonction des 1 dans le masque de sous-réseau. Cette propriété correspond à l'opérateur de bits <i>AND</i> avec <code>cfgRacTuneIpRangeMask</code> pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP contenant cette configuration binaire dans ses bits de niveau supérieur est autorisée à ouvrir une session. Les ouvertures de session à partir des adresses IP qui sont situées hors de cette plage échouent. Les valeurs par défaut de chaque propriété autorisent une plage d'adresses allant de 192.168.1.0 à 192.168.1.255 pour ouvrir une session.
<code>cfgRacTuneIpRangeMask</code>	Définit les positions binaires significatives dans l'adresse IP. Le masque doit avoir la forme d'un masque de réseau, où les bits les plus significatifs sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur.

Les exemples suivants utilisent la commande RACADM locale pour configurer le filtrage IP.

 **REMARQUE :** Consultez [Utilisation de l'interface de ligne de commande RACADM](#) pour plus d'informations sur la RACADM et les commandes RACADM.

1. Les commandes RACADM suivantes bloquent toutes les adresses IP sauf 192.168.0.57 :

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

2. Pour restreindre les ouvertures de session à un petit ensemble de quatre adresses IP adjacentes (par exemple, 192.168.0.212 à 192.168.0.215), sélectionnez tout, sauf les deux bits inférieurs dans le masque, comme illustré ci-dessous :

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 252.255.255.255
```

Le dernier octet du masque de plage est défini sur 252, l'équivalent décimal de 11111100b.

Instructions concernant le filtrage IP

Observez les instructions suivantes lorsque vous activez le filtrage IP :

1. Assurez-vous que `cfgRacTuneIpRangeMask` est configuré sous forme de masque de réseau, où tous les bits les plus significatifs sont des 1 (ce qui définit le sous-réseau dans le masque) avec une transition de tous les 0 dans les bits de niveau inférieur.
1. Utilisez l'adresse de base de la plage de votre choix comme valeur de `cfgRacTuneIpRangeAddr`. La valeur binaire de 32 bits de cette adresse doit avoir des zéros dans tous les bits de niveau inférieur où il y a des zéros dans le masque.

Configuration du blocage IP

Le blocage IP détermine de manière dynamique à quel moment un nombre excessif d'échecs d'ouverture de session se produit à partir d'une adresse IP particulière et empêche l'adresse de se connecter à iDRAC6 pendant une période prédéfinie.

Les fonctionnalités de blocage IP incluent :

1. Le nombre d'échecs d'ouverture de session autorisés (`cfgRacTuneIpBlkFailcount`)
1. Le laps de temps, en secondes, au cours duquel ces échecs doivent se produire (`cfgRacTuneIpBlkFailWindow`)
1. La durée, en secondes, pendant laquelle l'adresse IP bloquée ne peut établir une session lorsque le nombre d'échecs autorisés est dépassé (`cfgRacTuneIpBlkPenaltyTime`)

Étant donné que les échecs d'ouverture de session s'accumulent à partir d'une adresse IP spécifique, ils sont datés par un compteur interne. Lorsque l'utilisateur ouvre une session avec succès, l'historique des échecs est effacé et le compteur interne est remis à zéro.

 **REMARQUE :** Lorsque des tentatives d'ouverture de session sont refusées à partir de l'adresse IP client, certains clients SSH peuvent afficher le message suivant : `ssh exchange identification: Connection closed by remote host.` (identification d'échange ssh : connexion fermée par l'hôte distant).

Consultez le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals pour une liste complète des propriétés `cfgRacTune`.

[Tableau 13-5](#) répertorie les paramètres définis par l'utilisateur.

Tableau 13-5. Propriétés de restriction des nouvelles tentatives d'ouverture de session (blocage IP)

Propriété	Définition
-----------	------------

<code>cfgRacTuneIpBlkEnable</code>	Active la fonctionnalité de blocage IP. Lorsque des échecs consécutifs (<code>cfgRacTuneIpBlkFailCount</code>) à partir d'une seule adresse IP sont rencontrés pendant une période de temps spécifique (<code>cfgRacTuneIpBlkFailWindow</code>), tous les essais ultérieurs d'établissement d'une session à partir de cette adresse sont rejetés pour un certain temps (<code>cfgRacTuneIpBlkPenaltyTime</code>).
<code>cfgRacTuneIpBlkFailCount</code>	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.
<code>cfgRacTuneIpBlkFailWindow</code>	Le laps de temps, en secondes, au cours duquel les tentatives ayant échoué sont comptées. Lorsque le nombre d'échecs dépasse cette limite, les échecs sont déduits du compte.
<code>cfgRacTuneIpBlkPenaltyTime</code>	Définit la période, en secondes, pendant laquelle les tentatives d'ouverture de session à partir d'une adresse IP avec un nombre d'échecs excessif sont rejetées.

Activation du blocage IP

L'exemple suivant empêche une adresse IP client d'ouvrir une session pendant cinq minutes si ce client a échoué au cours de cinq tentatives d'ouverture de session en l'espace d'une minute.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

L'exemple suivant empêche plus de trois échecs de tentatives en l'espace d'une minute et empêche toute tentative d'ouverture de session supplémentaire pendant une heure.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

Configuration de services Telnet et SSH iDRAC6 via la RACADM locale

La console Telnet/SSH peut être configurée localement (sur le serveur géré) à l'aide des commandes RACADM.

 **REMARQUE :** Vous devez disposer de l'autorisation **Configurer iDRAC6** pour exécuter les commandes dans cette section.

 **REMARQUE :** Lorsque vous reconfigurez les paramètres Telnet ou SSH dans iDRAC6, toutes les sessions ouvertes prennent fin sans avertissement.

Pour activer Telnet et SSH depuis la commande RACADM locale, connectez-vous au serveur géré et entrez les commandes suivantes à l'invite de commande :

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

Pour désactiver le service Telnet ou SSH, remplacez la valeur 1 par 0 :

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0
racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Entrez la commande suivante pour changer le numéro du port Telnet iDRAC6 :

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <nouveau numéro de port>
```

Par exemple, pour modifier le port Telnet 23 par défaut et le définir sur 8022, entrez commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Pour obtenir la liste complète des commandes de CLI RACADM, consultez [Utilisation de l'interface de ligne de commande RACADM](#).

RACADM distante et SSH/Telnet

RACADM distante est un utilitaire côté client, qui peut être exécuté à partir d'une station de gestion via l'interface réseau hors bande. 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 est fournie. 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. RACADM SSH/Telnet est utilisée pour faire référence à l'utilisation de la commande RACADM à partir de l'invite SSH ou Telnet.

Le nombre maximal de sessions RACADM à distance simultanées autorisées est de quatre. Ces sessions sont indépendantes et en sus des sessions Telnet et SSH. iDRAC6 peut simultanément prendre en charge quatre sessions SSH et quatre sessions Telnet, en sus des quatre sessions RACADM.

 **REMARQUE :** Configurez l'adresse IP sur votre iDRAC6 avant d'utiliser la capacité d'accès à distance de la RACADM.

 **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.

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (Alerte de sécurité : le certificat est invalide : le nom sur le certificat est invalide ou ne correspond pas au nom du site)
```

```
Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors. (Continuer l'exécution. Utilisez l'option -S pour que la racadm interrompe l'exécution sur les erreurs liées au certificat).
```

La RACADM continue d'exécuter la commande. Toutefois, si vous utilisez l'option `-s`, la RACADM arrête d'exécuter la commande et affiche le message suivant :

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (Alerte de sécurité : le certificat est invalide : le nom sur le certificat est invalide ou ne correspond pas au nom du site)
```

```
Racadm not continuing execution of the command. (Racadm interrompt l'exécution de la commande).
```

ERROR: Unable to connect to iDRAC6 at specified IPaddress (ERREUR : Impossible de se connecter à iDRAC6 à l'adresse IP spécifiée)

 **REMARQUE :** Lorsque vous utilisez la capacité d'accès à distance de RACADM, vous devez posséder des droits d'écriture sur les dossiers sur lesquels vous utilisez les sous-commands RACADM impliquant des opérations sur des fichiers, par exemple :

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

ou

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

Utilisation de la RACADM distante

```
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 de l'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 distante

[Tableau 13-6](#) répertorie les options de la commande RACADM distante.

Tableau 13-6. Options de la commande RACADM

Option	Description
-r <racIpAddr>	Spécifie l'adresse IP distante du contrôleur.
-r <racIpAddr>:<numéro de port>	Utilisez <numéro de port> lorsque 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 <usrName>	Spécifie le nom d'utilisateur qui est utilisé pour authentifier la transaction de commande. Si l'option -u est utilisée, l'option -p doit être utilisée et l'option -i (interactive) n'est pas autorisée.
-p <mot de passe>	Spécifie le mot de passe utilisé pour authentifier la transaction de commande. Si l'option -p est utilisée, l'option -i n'est pas autorisée.
-S	Indique que la RACADM 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.

Utilisation d'un fichier de configuration iDRAC6

Un fichier de configuration iDRAC6 est un fichier texte contenant une représentation des valeurs dans la base de données iDRAC6. Vous pouvez utiliser la

sous-commande **getconfig RACADM** pour générer un fichier de configuration contenant les valeurs actuelles d'iDRAC6. Vous pouvez ensuite modifier le fichier et utiliser la sous-commande **config -f RACADM** pour recharger le fichier dans iDRAC6 ou pour copier la configuration sur d'autres iDRAC6.

Création d'un fichier de configuration iDRAC6

Le fichier de configuration est un fichier texte brut. Vous pouvez utiliser tout nom de fichier valide ; toutefois, l'extension de fichier **.cfg** est la convention recommandée.

Le fichier de configuration peut être :

- 1 créé à l'aide d'un éditeur de texte
- 1 obtenu auprès d'iDRAC6 avec la sous-commande **getconfig RACADM**
- 1 obtenu auprès d'iDRAC6 avec la sous-commande **getconfig RACADM** puis modifié

Pour obtenir un fichier de configuration, avec la commande **getconfig RACADM**, entrez la commande suivante :

```
racadm -r <IP iDRAC6 distant> -u <utilisateur> -p <mot de passe> getconfig -f myconfig.cfg
```

Cette commande crée le fichier **myconfig.cfg** dans le répertoire actuel.

Syntaxe du fichier de configuration

 **REMARQUE :** Modifiez le fichier de configuration à l'aide d'un éditeur de texte brut, tel que le **Bloc-notes** sous Windows ou **vi** sous Linux. L'utilitaire **racadm** analyse le texte ASCII uniquement. Tout formatage peut troubler l'analyseur et corrompre ainsi la base de données iDRAC6.

Cette section décrit le format du fichier de configuration.

- 1 Les lignes qui commencent par **#** sont des commentaires.

Un commentaire *doit* démarrer dans la première colonne de la ligne. Un caractère **#** dans toute autre colonne est traité comme un caractère **#** normal.

Exemple :

```
#  
  
# This is a comment (Il s'agit d'un commentaire)  
  
[cfgUserAdmin]  
  
cfgUserAdminPrivilege=4
```

- 1 Les entrées de groupe doivent être entourées de caractères **[** et **]**.

Le caractère **[** du début dénotant un nom de groupe *doit* commencer dans la colonne 1. Ce nom de groupe *doit* être spécifié avant n'importe quel objet dans ce groupe. Les objets auxquels aucun nom de groupe n'est associé génèrent une erreur. Les données de configuration sont organisées en groupes comme défini dans le *Guide de référence de l'administrateur d'iDRAC6* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

L'exemple suivant affiche un nom de groupe, un objet et la valeur de propriété de l'objet.

Exemple :

```
[cfgLanNetworking] (nom du groupe)  
  
cfgNicIpAddress=192.168.1.1 (nom de l'objet)
```

- 1 Les paramètres sont spécifiés en tant que paires *objet=valeur* sans espace entre l'objet, le signe **=** et la valeur.

Tout espace blanc inclus après la valeur est ignoré. L'espace blanc à l'intérieur d'une chaîne de caractères de valeur n'est pas modifié. Tout caractère à droite du signe **=** est pris tel quel (par exemple, un deuxième signe **=** ou un **#**, **[**, **]**, et ainsi de suite).

Pour afficher le contenu d'un groupe indexé, utilisez la commande suivante :

```
racadm getconfig -g <nom du groupe> -i <index>
```

- 1 Pour les groupes indexés, l'ancre d'objet *doit* être le premier objet après les crochets **[]**. Voici des exemples de groupes indexés actuels :

```
[cfgUserAdmin]  
  
cfgUserAdminIndex=11
```

- 1 Si l'analyseur rencontre un groupe indexé, l'index du groupe est utilisé comme ancre. Toutes les modifications apportées aux objets du groupe indexé sont également associées à la valeur d'index.

Par exemple :

```
[cfgUserAdmin]  
  
# cfgUserAdminIndex=11
```

```

cfgUserAdminUserName=

# cfgUserAdminPassword=***** (Write-Only)

cfgUserAdminEnable=0

cfgUserAdminPrivilege=0x00000000

cfgUserAdminIpmiLanPrivilege=15

cfgUserAdminIpmiSerialPrivilege=15

cfgUserAdminSolEnable=0

```

- 1 Les index sont en lecture seule et ne peuvent pas être modifiés. Les objets du groupe indexé sont liés à l'index sous lequel ils sont répertoriés et toute configuration valide de la valeur de l'objet s'applique uniquement à cet index-ci.
- 1 Un ensemble prédéfini d'index est disponible pour chaque groupe indexé. Pour plus d'informations, consultez le *Guide de référence de l'administrateur d'iDRAC* disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Modification de l'adresse IP iDRAC6 dans un fichier de configuration

Lorsque vous modifiez l'adresse IP iDRAC6 dans le fichier de configuration, supprimez toutes les entrées `<variable>=<valeur>` inutiles. Seul le nom du groupe variable actuel avec « [» et «] » reste avec les deux entrées `<variable>=<valeur>` correspondant au changement d'adresse IP.

Par exemple :

```

#

# Object Group (Groupe d'objet) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1

```

Ce fichier est mis à jour comme suit :

```

#

# Object Group (Groupe d'objet) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (commentaire, le reste de cette ligne est ignoré)

cfgNicGateway=10.35.9.1

```

Chargement du fichier de configuration dans iDRAC6

La commande `racadm config -f <nom de fichier>` analyse le fichier de configuration afin de s'assurer que des noms d'objet et de groupe valides sont présents et que les règles de syntaxe sont respectées. Si le fichier est exempt d'erreur, la commande met alors à jour la base de données iDRAC6 avec le contenu du fichier.

 **REMARQUE :** Pour vérifier la syntaxe uniquement et ne pas mettre à jour la base de données iDRAC6, ajoutez l'option `-c` à la sous-commande `config`.

Les erreurs détectées dans le fichier de configuration sont indiquées avec le numéro de ligne et un message qui explique le problème. Vous devez corriger toutes les erreurs pour que le fichier de configuration puisse mettre à jour iDRAC6.

 **REMARQUE :** Utilisez la sous-commande `racresetcfg` pour réinitialiser la base de données et les paramètres de carte d'interface réseau iDRAC6, et supprimer tous les utilisateurs et les configurations utilisateur. Pendant que l'utilisateur root est disponible, les paramètres par défaut des autres utilisateurs sont également réinitialisés.

Avant d'exécuter la commande `racadm config -f <nom de fichier>`, vous pouvez exécuter la sous-commande `racresetcfg` pour rétablir les paramètres par défaut de l'iDRAC6. Assurez-vous que le fichier de configuration que vous allez charger inclut tous les objets, utilisateurs, index et autres paramètres souhaités.

Pour mettre à jour iDRAC6 avec le fichier de configuration, exécutez la commande suivante :

```
racadm -r <IP iDRAC6 distant> -u <utilisateur> -p <mot de passe> config -f myconfig.cfg
```

Lorsque la commande s'est exécutée, vous pouvez exécuter la sous-commande `getconfig` RACADM pour confirmer que la mise à jour a réussi.

Configuration de plusieurs iDRAC6

À l'aide d'un fichier de configuration, vous pouvez configurer d'autres iDRAC6 avec des propriétés identiques. Suivez ces étapes pour configurer plusieurs iDRAC6 :

1. Créez le fichier de configuration de l'iDRAC6 dont vous souhaitez répliquer les paramètres vers les autres iDRAC. Entrez la commande suivante :

```
racadm -r <IP iDRAC6 distant> -u <utilisateur> -p <mot de passe> getconfig -f <nom de fichier>
```

où *<nom de fichier>* est le nom du fichier dans lequel sont enregistrées les propriétés iDRAC6, comme par exemple `myconfig.cfg`.

Les exemples ci-dessous montrent comment utiliser des commandes RACADM distantes pour configurer plusieurs iDRAC6. Créez un fichier séquentiel sur la station de gestion et appelez des commandes `racadm` distantes à partir du fichier séquentiel.

Par exemple :

```
racadm -r <IP du serveur 1> -u <utilisateur> -p <mot de passe> config -f myconfig.cfg
```

```
racadm -r <IP du serveur 2> -u <utilisateur> -p <mot de passe> config -f myconfig.cfg
```

...

Consultez la section [Création d'un fichier de configuration iDRAC6](#) pour plus d'informations.

 **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.

2. Modifiez le fichier de configuration que vous avez créé à l'étape précédente et supprimez ou commentez les paramètres que vous *ne voulez pas* répliquer.
3. Copiez le fichier de configuration modifié sur un lecteur réseau où il est accessible à chaque serveur géré pour lequel vous souhaitez configurer iDRAC6.
4. Pour chaque iDRAC6 que vous souhaitez configurer :

- a. Connectez-vous au serveur géré et démarrez une invite de commande.

- b. Si vous souhaitez reconfigurer iDRAC6 à partir des paramètres par défaut, entrez la commande suivante :

```
racadm racreset
```

- c. Chargez le fichier de configuration dans iDRAC6 à l'aide de la commande suivante :

```
racadm -r <IP iDRAC6 distant> -u <utilisateur> -p <mot de passe> config -f <nom de fichier>
```

où *<nom de fichier>* est le nom du fichier de configuration que vous avez créé. Incluez le chemin complet si le fichier ne se trouve pas dans le répertoire de travail.

- d. Réinitialisez l'iDRAC6 configuré en entrant la commande suivante :

```
racadm reset
```

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation de l'interface WS-MAN

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Fonctionnalités de WS-Management](#)
- [Profils CIM pris en charge](#)

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 organisées en profils, chacun définissant les interfaces spécifiques pour un domaine de gestion ou de fonctionnalité spécifique. 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 via WS-MAN sont fournies par l'interface d'instrumentation iDRAC6 adressée aux profils DMTF et aux profils d'extension Dell.

Fonctionnalités de WS-Management

La spécification WS-Management promeut l'interopérabilité entre les applications de gestion et les ressources gérées. En identifiant un ensemble principal de spécifications de services Web et d'exigences d'utilisation afin de présenter un ensemble commun d'opérations indispensables à tout système de gestion, WS-Management peut :

- 1 DÉTECTER la présence de ressources de gestion et naviguer entre elles ;
- 1 OBTENIR, DÉFINIR, CRÉER ET SUPPRIMER des ressources de gestion, tels que des paramètres et des valeurs dynamiques ;
- 1 ÉNUMÉRER le contenu de conteneurs et de collections, tels que de grands tableaux et journaux ;
- 1 EXÉCUTER des méthodes de gestion spécifiques avec des paramètres d'entrée et de sortie fortement typés.

Profils CIM pris en charge

Tableau 16-1. Profils CIM pris en charge

DMTF standard	
1.	Serveur de base Définit les classes CIM pour la représentation du serveur hôte.
2.	Mesures de base Définit les classes CIM pour fournir la capacité de modéliser et de contrôler les mesures capturées pour les éléments gérés.
3.	Processeur de service Définit les classes CIM pour la modélisation des processeurs de service.
4.	Redirection USB Définit les classes CIM pour la description des informations relatives aux redirections USB. Pour les claviers, les périphériques vidéo et les souris, ce profil doit être utilisé si les périphériques seront gérés comme des périphériques USB.
5.	Actif physique 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.
6.	Domaine d'administration SM-CLP Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP.
7.	Gestion de l'état de l'alimentation 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.
8.	Service CLP Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP.
9.	Interface IP Définit les classes CIM pour la représentation d'une interface IP d'un système géré.
10.	Cliant DHCP Définit les classes CIM pour la représentation d'un cliant DHCP et des capacités et de sa configuration associées.
11.	Cliant DNS Définit les classes CIM pour la représentation d'un cliant DNS au sein d'un système géré.

12.	Journal des enregistrements 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.	Autorisation basée sur les rôles Définit les classes CIM pour la représentation des rôles. iDRAC6 utilise ce profil pour configurer les privilèges de compte iDRAC6.
14.	Recueils SMASH Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP.
15.	Enregistrement des profils 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.
16.	Gestion simple des identités Définit les classes CIM pour la représentation des identités. iDRAC6 utilise ce profil pour configurer les comptes iDRAC6.
17.	Port Ethernet Définit les classes CIM pour la représentation d'un port Ethernet, du contrôleur qui lui est associé et des interfaces Ethernet au sein d'un système géré. Les associations avec l'aspect physique du port et les informations sur la version de l'implémentation de profil sont modélisées dans ce profil.
18.	Capteur Définit les classes CIM utilisées pour décrire les capteurs dans un système géré. Il définit également les classes d'association qui décrivent la relation entre les capteurs et les périphériques surveillés.
Extensions Dell	
1.	Client Active Directory 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 Définit les classes d'extension CIM et Dell pour la configuration du média virtuel iDRAC6. Étend le profil de <i>redirection USB</i> .
3.	Déploiement du SE 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.
4.	Inventaire des logiciels Définit les extensions CIM et Dell pour la représentation des versions actuellement installées du BIOS, du micrologiciel de composants, des diagnostics, d'Unified Server Configurator et de progiciels de pilotes. Représente également les versions des images de mise à jour du BIOS et du micrologiciel disponibles dans Lifecycle Controller à des fins de restauration et de réinstallation.
5.	Mise à jour de logiciels Définit les extensions CIM et Dell pour la représentation de la classe de service et des méthodes de mise à jour du micrologiciel du BIOS, des diagnostics, des progiciels de pilotes, de composants et de Lifecycle Controller. Les méthodes de mise à jour prennent en charge la mise à jour à partir des emplacements de partage réseau CIFS, NFS, FTP et HTTP et des images de mise à jour situées dans Lifecycle Controller. Les demandes de mise à jour sont formulées sous la forme de tâches et peuvent être programmées immédiatement ou ultérieurement avec un choix de types d'action de redémarrage pour appliquer les mises à jour.
6.	Contrôle des tâches Définit les extensions CIM et Dell pour gérer les tâches générées par les demandes de mise à jour. Les tâches peuvent être créées, supprimées, modifiées et agrégées en files d'attente de tâches afin de séquencer et d'effectuer plusieurs mises à jour au cours d'un seul redémarrage.
7.	Gestion de LC Définit les extensions CIM et Dell pour obtenir et définir des attributs pour gérer les fonctionnalités Découverte automatique et Pièces de rechange de Lifecycle Controller.
8.	Stockage permanent Définit les classes d'extensions CIM et Dell pour la gestion des partitions sur le média flash virtuel des plateformes Dell.
9.	NIC simple Définit les classes d'extensions CIM et Dell pour la représentation de la configuration des contrôleurs réseau NIC.
10.	Gestion du BIOS et du démarrage Définit les classes d'extensions CIM et Dell pour la représentation des attributs du BIOS Dell et pour la configuration de la séquence de démarrage de l'hôte.
11.	RAID simple Définit les classes d'extensions CIM et Dell pour la représentation de la configuration du stockage RAID de l'hôte.
12.	Carte iDRAC Définit les classes d'extensions CIM et Dell pour la représentation des informations d'inventaire d'iDRAC6.
13.	Mémoire Définit les classes d'extensions CIM et Dell pour la représentation des informations d'inventaire DIMM de l'hôte.
14.	UC

Définit les classes d'extensions CIM et Dell pour la représentation des informations d'inventaire d'UC de l'hôte.
15. Infos du système Définit les classes d'extensions CIM et Dell pour la représentation des informations d'inventaire de la plateforme hôte.
16. Périphérique PCI Définit les classes d'extensions CIM et Dell pour la représentation des informations d'inventaire du périphérique PCI de l'hôte.
17. Vidéo Définit les classes d'extensions CIM et Dell pour la représentation des informations d'inventaire de la carte vidéo de l'hôte.

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 telle que Windows WinRM et la CLI Powershell, les utilitaires open source comme WSMANCLI et les environnements de programmation d'application tels que Microsoft .NET.

Des guides de mise en œuvre, des livres blancs, des profils, des MOF 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 :

- 1 Le Site Web de DMTF : www.dmtf.org/standards/profiles/
- 1 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 d'iDRAC6 Enterprise Interface de ligne de commande SM-CLP

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [System Management avec SM-CLP](#)
- [Prise en charge de SM-CLP iDRAC6](#)
- [Fonctionnalités de SM-CLP](#)
- [Navigation dans l'espace d'adressage MAP](#)
- [Utilisation du verbe Show](#)
- [Exemples de SM-CLP iDRAC6](#)

Cette section fournit des informations sur le protocole de ligne de commande Server Management (SM-CLP) du groupe de travail Server Management (SMWG) intégré à iDRAC6.

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

SM-CLP iDRAC6 est un protocole régi par DMTF et SMWG pour fournir des normes aux implémentations CLI de gestion de systèmes. De nombreux efforts ont été accomplis par une architecture SMASH définie qui doit servir de base à un ensemble de composants de gestion de systèmes plus normalisé. SMWG SM-CLP est un sous-composant de l'ensemble des efforts SMASH effectués par DMTF.

L'interface SM-CLP intègre un sous-ensemble des fonctionnalités fournies par l'interface de ligne de commande RACADM locale, mais avec un chemin d'accès différent. L'interface SM-CLP s'exécute au sein d'iDRAC6, tandis que la RACADM s'exécute sur le serveur géré. En outre, la RACADM est une interface propriétaire Dell, tandis que SM-CLP est une interface standard du secteur.

 **REMARQUE :** Pour plus d'informations sur la base de données de propriétés SM-CLP iDRAC6, l'adressage entre les classes WS-MAN et les cibles SM-CLP, et des informations détaillées sur l'implémentation Dell, consultez les documents *iDRAC6 CIM Element Mapping* et *iDRAC6 SM-CLP Property Database* disponibles dans le centre Dell Enterprise Technology Center à l'adresse www.delltechcenter.com. Les informations incluses dans le document *iDRAC6 CIM Element Mapping* sont spécifiées dans les profils DMTF et dans les extensions de Dell à ces profils. Les structures WSMAN sont documentées dans les profils DMTF et les MOF disponibles à l'adresse <http://www.dmtf.org/standards/profiles/>. En outre, des extensions Dell sont disponibles à l'adresse <http://www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions>.

System Management avec SM-CLP

L'interface SM-CLP iDRAC6 vous permet de gérer les fonctionnalités système suivantes à partir d'une ligne de commande :

- 1 Gestion de l'alimentation du serveur : met sous tension, arrête ou redémarre le système
- 1 Gestion du journal des événements système (SEL) : affiche ou efface les enregistrements du journal SEL
- 1 Gestion de compte utilisateur iDRAC6
- 1 Configuration d'Active Directory
- 1 Configuration du LAN iDRAC6
- 1 Génération de la requête de signature de certificat (RSC) SSL
- 1 Configuration du média virtuel

Prise en charge de SM-CLP iDRAC6

L'interface SM-CLP est hébergée par le micrologiciel iDRAC6 et prend en charge les connexions Telnet et SSH. L'interface SM-CLP iDRAC6 repose sur la spécification SM-CLP, version 1.0, fournie par l'organisation DMTF.

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

 **REMARQUE :** Si vous avez établi une session SM-CLP via Telnet/SSH et que la session ne se ferme pas correctement en raison de la déconnexion du réseau, un message indiquant que vous avez atteint le nombre maximum de connexions peut s'afficher. Pour résoudre ce problème, terminez la session SM-CLP dans l'interface utilisateur Web dans **Système** → **Accès à distance** → **iDRAC6** → **Réseau/Sécurité** → **Sessions** avant d'essayer d'en établir une nouvelle.

 **REMARQUE :** iDRAC6 prend en charge jusqu'à 4 sessions Telnet et 4 sessions SSH simultanément. Cependant, uniquement *une* de ces 8 sessions potentielles peut utiliser SM-CLP. En d'autres termes, iDRAC6 prend en charge uniquement une session SM-CLP à la fois.

Comment démarrer une session SM-CLP

- 1 Connectez-vous à iDRAC6 via SSH/Telnet qui vous conduit à l'interface de ligne de commande (console).
- 1 Entrez « smclp » à l'invite dollar afin de lancer la console SM-CLP.

Syntaxe :

```
telnet <adresse IP iDRAC6>
$ (the CLI prompt is displayed)(l'invite CLI s'affiche)
$smclp (at the CLI prompt, type smclp)(dans l'invite CLI, tapez smclp)
```

Fonctionnalités de SM-CLP

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

SM-CLP encourage la conception de verbes et de cibles pour fournir des capacités de configuration de systèmes via la CLI. Le verbe indique l'opération à effectuer et la cible est l'entité (ou l'objet) sur laquelle l'opération est exécutée.

La syntaxe suivante s'applique à la ligne de commande SM-CLP :

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

[Tableau 15-1](#) fournit la liste des verbes pris en charge par l'interface de ligne de commande iDRAC6, la syntaxe de chaque commande et la liste des options prises en charge par le verbe.

Tableau 15-1. Verbes d'interface de ligne de commande SM-CLP pris en charge

Verbe	Description	Options
cd	Navigue dans l'espace d'adressage du système géré via l'environnement. Syntaxe : cd [options] [cible]	-default, -examine, -help, -output, -version
delete	Supprime une instance d'objet. Syntaxe : delete [options] cible	-examine, -help, -output, -version
exit	Quitte la session d'environnement SM-CLP. Syntaxe : exit [options]	-help, -output, -version
help	Affiche l'aide pour les commandes SM-CLP. help	-examine, -help, -output, -version
reset	Réinitialise la cible. Syntaxe : reset [options] [cible]	-examine, -help, -output, -version
set	Définit les propriétés d'une cible Syntaxe : set [options] [cible] <nom de propriété>=<valeur>	-examine, -help, -output, -version
show	Affiche les propriétés, les verbes et les sous-cibles de la cible. Syntaxe : show [options] [cible] <nom de propriété>=<valeur>	-all, -default, -display, -examine, -help, -level, -output, -version
start	Démarre une cible. Syntaxe : start [options] [cible]	-examine, -force, -help, -output, -version
stop	Désactive une cible. Syntaxe : stop [options] [cible]	-examine, -force, -help, -output, -version, -wait
version	Affiche les attributs de version d'une cible. Syntaxe : version [options]	-examine, -help, -output, -version

[Tableau 15-2](#) décrit les options SM-CLP. Certaines options ont des formes abrégées, comme indiqué dans le tableau.

Tableau 15-2. Options SM-CLP prises en charge

Option SM-CLP	Description
-all, -a	Ordonne au verbe d'exécuter toutes les fonctionnalités possibles.
-destination	Spécifie l'emplacement de stockage d'une image dans la commande dump. Syntaxe : -destination <URI>
-display, -d	Filtre le résultat de la commande. Syntaxe : -display <propriétés cibles verbes>[, <propriétés cibles verbes>]*
-examine, -x	Ordonne au processeur de commandes de valider la syntaxe de commande sans exécuter la commande.
-force, -f	Si l'arrêt normal n'aboutit pas, utilisez cette option pour effectuer un arrêt forcé du système cible. Syntaxe : stop -force <cible>
-help, -h	Affiche l'aide pour le verbe.
-level, -l	Ordonne au verbe d'agir sur les cibles à des niveaux supplémentaires sous la cible spécifiée. Syntaxe : -level <n all>
-output, -o	Spécifie le format de la sortie. Syntaxe : -output format=<texte clpcsv mot clé clpxml> ou -o format=<texte clpcsv mot clé clpxml>
-version, -v	Affiche le numéro de version SM-CLP.

Navigation dans l'espace d'adressage MAP

 **REMARQUE :** La barre oblique (/) et la barre oblique inverse (\) sont interchangeables dans les chemins d'adresse SM-CLP. Toutefois, une barre oblique inverse située à la fin d'une ligne de commande permet de continuer la commande à la ligne suivante et est ignorée lorsque la commande est analysée.

Les objets pouvant être gérés via SM-CLP sont représentés par des cibles disposées dans un espace hiérarchique appelé espace d'adressage MAP (Manageability Access Point). Un chemin d'adresse spécifie le chemin de la racine de l'espace d'adressage vers un objet dans l'espace d'adressage.

La cible racine est représentée par une barre oblique (/) ou une barre oblique inverse (\). Il s'agit du point de démarrage par défaut lorsque vous ouvrez une session iDRAC6. Naviguez à partir de la racine à l'aide du verbe `cd`.

Par exemple, pour naviguer vers le troisième enregistrement du journal des événements système (SEL), entrez la commande suivante :

```
->cd /admin/system1/logs1/log1/record3
```

Entrez le verbe `cd` sans cible pour trouver votre emplacement actuel dans l'espace d'adressage. Les abréviations `..` et `.` fonctionnent de la même manière que sous Windows et Linux : `..` fait référence au niveau parent et `.` fait référence au niveau actuel.

Cibles

Pour obtenir une liste des cibles disponibles dans l'interface SM-CLP, consultez le document SM-CLP Mapping disponible dans le centre Dell Enterprise Technology Center à l'adresse www.delltechcenter.com.

Utilisation du verbe Show

Pour en savoir plus sur une cible, utilisez le verbe `show`. Ce verbe affiche les propriétés de la cible, les sous-cibles, les associations et une liste des verbes SM-CLP autorisés à cet emplacement.

Utilisation de l'option -display

L'option **show -display** vous permet de restreindre la sortie de la commande à un(e) ou plusieurs propriétés, cibles, associations et verbes. Par exemple, pour afficher uniquement les propriétés et cibles à l'emplacement actuel, utilisez la commande suivante :

```
show -display properties,targets
```

Pour répertorier uniquement certaines propriétés, qualifiez-les, comme dans la commande suivante :

```
show -d properties=(userid,name) /admin1/system1/spl/oemdcim_mfaaccount1
```

Si vous souhaitez uniquement afficher une propriété, vous pouvez omettre les parenthèses.

Utilisation de l'option -level

L'option **show -level** exécute le verbe **show** sur les niveaux supplémentaires sous la cible spécifiée. Pour afficher toutes les cibles et propriétés de l'espace d'adressage, utilisez l'option **-l all**.

Utilisation de l'option -output

L'option **-output** spécifie l'un des quatre formats de sortie suivants pour les verbes SM-CLP : **texte**, **clpcsv**, **mot clé** et **clpxml**.

Le format **texte** est le format par défaut ; il s'agit de la sortie la plus lisible. Le format **clpcsv** est un format de valeurs séparées par une virgule approprié au chargement dans un tableur. Le format **mot clé** sort des informations sous forme de liste de paires mot clé=valeur, une par ligne. Le format **clpxml** est un document XML contenant un élément XML de **réponse**. DMTF a spécifié les formats **clpcsv** et **clpxml**, et leurs spécifications sont disponibles sur le site Web DMTF à l'adresse www.dmtf.org.

L'exemple suivant montre comment faire apparaître le contenu du journal SEL au format XML :

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Exemples de SM-CLP iDRAC6

La sous-section suivante fournit des exemples quant à la manière de se connecter à iDRAC6 via l'interface SSH et d'ouvrir une session SM-CLP pour effectuer les opérations suivantes :

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

Gestion de l'alimentation du serveur

[Tableau 15-3](#) fournit des exemples d'utilisation de SM-CLP pour effectuer des opérations de gestion de l'alimentation sur un serveur géré.

Entrez « **smclp** » pour lancer la console SM-CLP.

Tableau 15-3. Opérations de gestion de l'alimentation du serveur

Opération	Syntaxe
Connexion à iDRAC6 via l'interface SSH	>ssh 192.168.0.120 >login: root >password: Entrez « smclp » pour lancer la console SM-CLP.
Mettre le serveur hors tension	->stop /admin1/system1 system1 correctement arrêté
Mettre le serveur sous tension à partir de l'état hors tension	->start /admin1/system1 system1 successfully started
Redémarrer le serveur	->reset /admin1/system1 RESET successful for system1

Gestion du journal SEL

[Tableau 15-4](#) fournit des exemples d'utilisation de SM-CLP pour effectuer des opérations liées au journal SEL sur le système géré.

Navigation de la cible MAP

Tableau 15-4. Opérations de gestion du journal SEL

Opération	Syntaxe
Affichage du journal SEL	<pre>->show -d targets,properties,verbs /admin1/system1/logs1/log1</pre> <p>Peut renvoyer : Cibles : record1/ record2/...</p> <p>Properties: OverwritePolicy=7</p> <p>LogState=4</p> <p>CurrentNumberOfRecords=60</p> <p>MaxNumberOfRecords=512</p> <p>ElementName=Record Log 1</p> <p>HealthState=5</p> <p>EnabledState=2</p> <p>RequestedState=12</p> <p>EnabledDefault=2</p> <p>TransitioningToState=12</p> <p>InstanceID=DCIM: SEL Log</p> <p>OperationalStatus={2}</p> <p>Verbes : show exit version cd help</p>
Affichage de l'enregistrement du journal SEL	<pre>->show /admin1/system1/logs1/log1/record4</pre> <p>Peut renvoyer : ufip=/admin1/system1/logs1/log1/record4</p> <p>Associations:LogManagesRecord=>/admin1/system1/logs1/log1</p> <p>Properties :</p> <p>RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255*</p> <p>RecordFormat=*IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*IPMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI_GeneratorID*IPMI_EvM</p> <p>Description=:0:Assert:OEM specific</p> <p>ElementName=DCIM System Event Log Entry</p> <p>InstanceID=DCIM:SEL LOG:4</p> <p>LogInstanceID=idrac:Unknown:Unknown SEL Log</p> <p>LogName=DCIM System Event Log Entry</p> <p>RecordID=DCIM:SEL LOG:4</p> <p>CreationTimeStamp=20090616114341.000000+000</p>
	<p>Verbes : show exit version cd help delete</p>

Effacement du journal SEL ->delete /admin1/system1/logs1/log1/record*

Renvoie :
Records deleted successfully.(Enregistrements correctement supprimés).

[Tableau 15-5](#) fournit des exemples d'utilisation du verbe **cd** pour naviguer dans MAP. Dans tous les exemples, la cible par défaut initiale est supposée être /.

Tableau 15-5. Opérations de navigation de la cible MAP

Opération	Syntaxe
Naviguer vers la cible système et redémarrer	->cd admin1/system1 ->reset REMARQUE : La cible par défaut actuelle est /.
Naviguer vers la cible SEL et afficher les enregistrements du journal	->cd admin1 ->cd system1 ->cd logs1 ->cd log1 ->show équivalent à ->cd admin1/system1/logs1/log1 ->show
Afficher la cible actuelle	->cd .
Monter d'un niveau	->cd ..
Quitter l'environnement	->exit

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Déploiement de votre système d'exploitation via iVMCLI

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Avant de commencer](#)
- [Création d'un fichier image d'amorçage](#)
- [Préparation au déploiement](#)
- [Déploiement du système d'exploitation](#)
- [Utilisation de l'utilitaire d'interface de ligne de commande de média virtuel](#)

L'utilitaire d'interface de ligne de commande de média virtuel intégré (iVMCLI) 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 l'utilitaire iVMCLI et de méthodes cryptées, vous pouvez déployer votre système d'exploitation sur plusieurs systèmes distants au sein de votre réseau.

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

Avant de commencer

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

Exigences du système distant

- 1 iDRAC6 est configuré dans chaque système distant.

Configuration réseau requise

Un partage réseau doit comprendre les composants suivants :

- 1 Fichiers de système d'exploitation
- 1 Pilotes requis
- 1 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 d'amorçage

Avant de déployer votre fichier image sur les systèmes distants, assurez-vous qu'un système pris en charge peut être démarré à partir du fichier. Pour tester le fichier image, transférez-le vers un système de test à l'aide de l'interface utilisateur Web iDRAC6, puis redémarrez le système.

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

Création d'un fichier image pour les systèmes Linux

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

Pour exécuter l'utilitaire, ouvrez une invite de commande et entrez 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 répliqueur 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 d'amorçage préconfiguré pour déployer le système d'exploitation sur les systèmes distants, ignorez cette étape.

Si vous n'avez pas de fichier image de déploiement d'amorçage 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 Microsoft Windows, le fichier image peut inclure des programmes qui sont semblables aux méthodes de déploiement utilisées par Microsoft Systems Management Server (SMS).

Lorsque vous créez le fichier image, procédez comme suit :

- 1 Suivez les procédures d'installation réseau standard.
 - 1 Mettez l'image de déploiement en « lecture seule » pour garantir que chaque système cible démarre et exécute la même procédure de déploiement.
- 1 Effectuez l'une des procédures suivantes :
 - 1 Intégrez **IPMI tool** et l'interface de ligne de commande de média virtuel (**iVMCLI**) dans votre application de déploiement de système d'exploitation existante. Utilisez l'exemple de script **ivmdeploy** comme guide d'utilisation de l'utilitaire.
 - 1 Utilisez le script **ivmdeploy** existant pour déployer votre système d'exploitation.

 **REMARQUE :** **ivmdeploy** utilise en interne **iVMCLI** et **ipmitool**. Vous devez disposer du privilège *IPMI sur le LAN* pour utiliser cet outil. En outre, le média virtuel doit être connecté lors de l'utilisation du script **ivmdeploy**.

Déploiement du système d'exploitation

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

Avant de commencer, vérifiez l'exemple de script **ivmdeploy** inclus avec l'utilitaire **iVMCLI**. 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 IP iDRAC6 des systèmes distants qui seront déployés dans le fichier texte **ip.txt**, en indiquant une adresse IP par ligne.
2. Insérez un CD ou un DVD de système d'exploitation d'amorçage dans le lecteur de média client.
3. Exécutez **ivmdeploy** à la ligne de commande.

Pour exécuter le script **ivmdeploy**, entrez la commande suivante à l'invite de commande :

```
ivmdeploy -r ip.txt -u <utilisateur idrac> -p <mot de passe idrac> -c {<image iso9660> | <chemin>}
```

où :

- 1 <utilisateur idrac> est le nom d'utilisateur iDRAC6, par exemple **root**
- 1 <mot de passe idrac> est le mot de passe de l'utilisateur iDRAC6, par exemple **calvin**
- 1 <image iso9660> est le chemin d'une image ISO9660 du CD ou du DVD d'installation du système d'exploitation
- 1 <chemin> est le chemin d'accès au périphérique contenant le CD ou DVD d'installation du système d'exploitation

Le script **ivmdeploy** transmet ses options de ligne de commande à l'utilitaire **iVMCLI**. 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 **iVMCLI -r**. Si l'argument de l'option **-r** est le nom d'un fichier existant, le script lit les adresses IP iDRAC6 du fichier spécifié et exécute l'utilitaire **iVMCLI** à une seule reprise pour chaque ligne. Si l'argument de l'option **-r** n'est pas un nom de fichier, il doit correspondre à l'adresse d'un iDRAC6 unique. Dans ce cas, l'option **-r** fonctionne comme décrit pour l'utilitaire **iVMCLI**.

Le script **ivmdeploy** prend en charge l'installation uniquement à partir d'un CD/DVD ou d'une image ISO9660 de CD/DVD. Si vous devez procéder à l'installation à partir d'une disquette ou d'une image de disquette, vous pouvez modifier le script pour utiliser l'option **iVMCLI -f**.

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

L'utilitaire d'interface de ligne de commande de média virtuel (**iVMCLI**) est une interface de ligne de commande pouvant contenir des scripts qui fournissent les fonctionnalités de média virtuel de la station de gestion à iDRAC6.

L'utilitaire **iVMCLI** fournit les fonctionnalités suivantes :

 **REMARQUE :** Lors de la virtualisation de fichiers image en lecture seule, plusieurs sessions peuvent partager le même média image. Lors de la virtualisation de lecteurs physiques, une seule session peut accéder à un lecteur physique donné à la fois.

- 1 Les périphériques de média amovibles ou les fichiers image qui sont en accord avec les plug-in du média virtuel
- 1 L'arrêt automatique lorsque l'option de démarrage unique du micrologiciel iDRAC6 est activée
- 1 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 pouvoir exécuter iDRAC6.

 **PRÉCAUTIONS :** Il est recommandé d'utiliser l'option « -i » d'indicateur interactif lors du démarrage de l'utilitaire de ligne de commande iVMCLI. Ceci renforce la sécurité en gardant le nom d'utilisateur et le mot de passe privés, car sur de nombreux systèmes d'exploitation Windows et Linux, le nom d'utilisateur et le mot de passe apparaissent en texte en clair lorsque les processus sont examinés par d'autres utilisateurs.

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

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

Pour les systèmes Windows, vous devez disposer des droits d'utilisateur privilégié pour pouvoir exécuter l'utilitaire iVMCLI.

Pour les systèmes Linux, vous pouvez accéder à l'utilitaire iVMCLI sans privilèges d'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 iVMCLI, l'administrateur utilise la commande **visudo**. Les utilisateurs sans privilèges d'administrateur peuvent ajouter la commande **sudo** comme préfixe à la ligne de commande iVMCLI (ou au script iVMCLI) afin d'accéder à iDRAC6 dans le système distant et d'exécuter l'utilitaire.

Installation de l'utilitaire iVMCLI

L'utilitaire iVMCLI se trouve sur le DVD *Dell Systems Management Tools and Documentation* qui est inclus avec votre kit logiciel Dell OpenManage System Management. Pour installer l'utilitaire, insérez le DVD dans votre système, puis suivez les instructions qui s'affichent à l'écran.

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

De plus, le DVD *Dell Systems Management Tools and Documentation* inclut **ivmdeploy**, un modèle de script qui illustre comment utiliser les utilitaires iVMCLI et RACADM pour déployer le logiciel sur plusieurs systèmes distants.

 **REMARQUE :** Le script **ivmdeploy** dépend des autres fichiers présents dans son répertoire lors de son installation. Si vous souhaitez utiliser le script à partir d'un autre répertoire, copiez tous les fichiers présents dans ce dernier.

Options de ligne de commande

L'interface iVMCLI est identique sur les systèmes Linux et Windows. L'utilitaire utilise des options qui sont en accord avec les options de l'utilitaire RACADM. Par exemple, une option pour spécifier l'adresse IP iDRAC6 exige la même syntaxe tant pour la RACADM que pour les utilitaires iVMCLI.

Le format d'une commande iVMCLI est comme suit :

```
iVMCLI [paramètre] [options d'environnement de système d'exploitation]
```

La syntaxe de ligne de commande est sensible à la casse. Consultez la section [Paramètres iVMCLI](#) pour plus d'informations.

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 :

- 1 La connexion iVMCLI est interrompue pour une raison ou une autre.
- 1 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.

 **REMARQUE :** Lorsque vous utilisez la commande iVMCLI, si les valeurs de paramètres comportent des espaces entre les mots, vous devez utiliser des guillemets pour la valeur complète du paramètre. Par exemple, prenez la commande visant à associer l'image d'un DVD entre votre système et le système d'exploitation du serveur :

```
F:\idrac>ivmcli -r 10.35.155.117 -u root -p calvin -c c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso
```

où -c est l'un des paramètres et c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso correspond à la valeur du paramètre qui contient des espaces pour « documents and settings » et pour « my documents ». Les guillemets sont ainsi utilisés pour le chemin complet du fichier image. Sans les guillemets, la commande n'aboutit pas. L'exemple ci-dessous est également non valide :

```
C:\>"documents and settings"\.....\
```

Paramètres iVMCLI

Adresse IP iDRAC6

```
-r <adresse IP iDRAC6>[:<port SSL iDRAC6>]
```

Ce paramètre fournit l'adresse IP iDRAC6 et le port SSL pour lesquels l'utilitaire doit établir une connexion de média virtuel avec l'iDRAC6 cible. Si vous saisissez une adresse IP ou un nom DDNS non valide, un message d'erreur apparaît et la commande est terminée.

<adresse IP iDRAC6> est une adresse IP unique valide ou le nom DDNS (Dynamic Domain Naming System) iDRAC6 (si pris en charge). Si le <port SSL iDRAC6> est omis, le port 443 (port par défaut) est utilisé. À moins que le port SSL par défaut iDRAC6 n'ait été modifié, le port SSL optionnel n'est pas obligatoire.

Nom d'utilisateur iDRAC6

-u <nom d'utilisateur iDRAC6>

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

Le <nom d'utilisateur iDRAC6> doit avoir les attributs suivants :

- 1 Nom d'utilisateur valide
- 1 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-iDRAC6>

Ce paramètre fournit le mot de passe de l'utilisateur iDRAC6 spécifié.

Si l'authentification iDRAC6 échoue, un message d'erreur s'affiche et la commande se termine.

Périphérique de disquette/disque ou fichier image

-f {<nom de périphérique> | <fichier image>}

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

Ce paramètre spécifie le périphérique ou le fichier qui fournit le média de disquette/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 # 4th partition on device /dev/sdb (4ème partition sur le périphérique /dev/sdb) (système Linux)

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

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

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.

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

Par exemple, un fichier image est spécifié comme :

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

-c /tmp/mydvd.img (systèmes Linux)

Par exemple, un périphérique est spécifié comme :

-c d:\ (systèmes Windows)

-c/dev/cdrom (systèmes Linux)

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

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

Validation du certificat d'une autorité de certification racine

-s

Ce paramètre sert à indiquer si le certificat d'une autorité de certification iDRAC est valide ou non. Si le certificat n'est pas valide, la session iVMCLI est clôturée et un message d'erreur s'affiche pour indiquer que le certificat n'est pas valide. Si le certificat est valide, la session iVMCLI est établie.

Affichage de la version

-v

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

Affichage de l'aide

-h

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

Affichage manuel

-m

Ce paramètre affiche une « page manuelle » détaillée pour l'utilitaire iVMCLI, incluant les descriptions de toutes les options possibles.

Données cryptées

-e

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

Options d'environnement du système d'exploitation iVMCLI

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

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

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

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

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

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

Codes de retour iVMCLI

0 = aucune erreur

1 = connexion impossible

2 = erreur de ligne de commande iVMCLI

3 = connexion du micrologiciel du RAC coupée

Les messages de texte (en anglais seulement) sont également 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](#)

Utilisation de l'utilitaire de configuration iDRAC6

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [Présentation](#)
- [Démarrage de l'utilitaire de configuration iDRAC6](#)
- [Utilisation de l'utilitaire de configuration iDRAC6](#)

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 système géré. Vous pouvez notamment :

- 1 afficher les numéros de révision du micrologiciel pour iDRAC6 et le micrologiciel de fond de panier principal
- 1 configurer, activer ou désactiver le réseau local iDRAC6
- 1 activer ou désactiver IPMI sur le LAN
- 1 configurer les paramètres LAN
- 1 activer, désactiver ou annuler les services système
- 1 activer ou désactiver la découverte automatique et configurer le serveur de d'approvisionnement
- 1 connecter ou déconnecter les périphériques Média virtuel
- 1 activer ou désactiver vFlash
- 1 activer ou désactiver la connexion par carte à puce et la connexion directe
- 1 configurer les services système
- 1 changer le nom d'utilisateur et le mot de passe d'administration
- 1 rétablir les paramètres d'usine de la configuration iDRAC6
- 1 afficher ou effacer les messages du journal des événements système (SEL)

Les tâches que vous pouvez effectuer à l'aide de l'utilitaire de configuration iDRAC6 peuvent également être effectuées via d'autres utilitaires fournis par iDRAC6 ou le logiciel Dell OpenManage, notamment l'interface Web, l'interface de ligne de commande SM-CLP, l'interface de ligne de commande RACADM locale et distante et, dans le cas de la configuration réseau de base, sur l'écran LCD d'iDRAC6 lors de la configuration initiale d'iDRAC6.

Démarrage de l'utilitaire de configuration iDRAC6

Vous devez utiliser une console connectée à la console virtuelle iDRAC6 pour accéder initialement à l'utilitaire de configuration iDRAC6 ou après une réinitialisation des paramètres par défaut d'iDRAC6.

1. Sur le clavier connecté à la console virtuelle iDRAC6, appuyez sur <Impr. écran> pour afficher le menu **OSCAR (On Screen Configuration and Reporting)** d'iDRAC6. Utilisez la <flèche vers le haut> et la <flèche vers le bas> pour mettre en surbrillance le logement contenant votre serveur, puis appuyez sur <Entrée>.
2. Mettez sous tension ou redémarrez le serveur en appuyant sur le bouton d'alimentation situé à l'avant du serveur.
3. Lorsque le message **Press <Ctrl-E> for Remote Access Setup within 5sec (Appuyez sur <Ctrl-E> pour configurer l'accès à distance dans 5 sec)...** s'affiche, appuyez immédiatement sur <Ctrl><E>. L'utilitaire de configuration iDRAC6 s'affiche.

 **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.

Les deux premières lignes de l'utilitaire de configuration fournissent des informations sur le micrologiciel iDRAC6 et les révisions du micrologiciel de 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 du micrologiciel s'articulant autour des interfaces externes, telles que l'interface Web, les interfaces SM-CLP et Web. Le micrologiciel de fond de panier principal est la partie du micrologiciel qui s'interface avec l'environnement matériel du serveur et qui le surveille.

Utilisation de l'utilitaire de configuration iDRAC6

Sous les messages de révision du micrologiciel, le reste de l'utilitaire de configuration iDRAC6 se compose d'un menu d'éléments auxquels vous pouvez accéder à l'aide de la flèche vers le haut et de la flèche vers le bas.

- 1 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.
- 1 Si des valeurs sélectionnables telles que **Oui/Non** ou **Activé/Désactivé** sont associées à un élément, appuyez sur la flèche gauche, la flèche droite ou sur Espace pour choisir une valeur.

- 1 Si un élément n'est pas modifiable, il apparaît en bleu. Certains éléments deviennent modifiables en fonction des autres sélections que vous effectuez.
- 1 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.
- 1 Lorsque vous avez fini d'utiliser l'utilitaire de configuration iDRAC6, appuyez sur <Échap> pour afficher le menu Quitter, dans lequel vous pouvez choisir d'enregistrer ou d'ignorer vos modifications, ou encore de retourner dans l'utilitaire.

Les sections suivantes décrivent les éléments de menu de l'utilitaire de configuration iDRAC6.

LAN iDRAC6

Utilisez la flèche gauche, la flèche droite et la barre d'espace pour choisir entre **Activé** et **Désactivé**.

Le LAN iDRAC6 est désactivé dans la configuration par défaut. Le réseau local doit être activé pour permettre l'utilisation des services iDRAC6, comme l'interface Web, l'accès Telnet/SSH à l'interface de ligne de commande SM-CLP, la console virtuelle et le média virtuel.

Si vous choisissez de désactiver le LAN, l'avertissement suivant s'affiche :

iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (L'interface hors bande iDRAC sera désactivée si le canal LAN est désactivé).

Le message vous informe que, outre les services auxquels vous accédez en vous connectant directement aux ports iDRAC6 HTTP, HTTPS, Telnet ou SSH, le trafic réseau de gestion hors bande, tels que les messages IPMI envoyés à iDRAC6 à partir d'une station de gestion, n'est pas reçu lorsque le LAN est désactivé. L'interface RACADM locale reste disponible et peut être utilisée pour reconfigurer le LAN iDRAC6.

Appuyez sur n'importe quelle touche pour effacer le message et continuer.

IPMI sur le LAN

Appuyez sur la flèche gauche, la flèche droite et la barre d'espace pour choisir entre **Activé** et **Désactivé**. Lorsque **Désactivé** est sélectionné, iDRAC6 n'accepte pas les messages IPMI en provenance de l'interface LAN.

Si vous sélectionnez **Désactivé**, un message d'avertissement s'affiche.

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	
Adresse Mac	Il s'agit de l'adresse MAC non modifiable de l'interface réseau iDRAC6.
Activation du VLAN	Affiche Activé/Désactivé . Activé activera le filtrage du réseau local virtuel pour iDRAC6.
N° VLAN	Affiche une valeur de référence du VLAN, comprise entre 1 et 4 094.
VLAN	Indique la priorité du VLAN, comprise 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 accéder au nom iDRAC6 dans DNS.
Nom iDRAC6	Si Inscrire 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 <i>masociété.com</i> .
Chaîne de nom d'hôte	Appuyez sur <Entrée> pour modifier. Saisissez le nom de l'hôte pour les alertes PET (Platform Event Trap [interruption d'événement sur plateforme]).
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. Activé est sélectionné par défaut.
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. Lorsque Statique est sélectionné, les éléments Adresse IP Ethernet , Masque de sous-réseau et Passerelle par défaut deviennent modifiables.
Adresse IP Ethernet	Si la source d'adresse IP est définie sur DHCP , ce champ affiche l'adresse IP obtenue auprès de DHCP. Si la source d'adresse IP est définie sur Statique , entrez l'adresse IP que vous souhaitez attribuer à iDRAC6. 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. Si la source d'adresse IP est définie sur Statique , entrez 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. Si la source d'adresse IP est définie sur Statique , entrez l'adresse IP de la passerelle par défaut. L'adresse par défaut est 192.168.0.1 .
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 , entrez l'adresse IP du premier serveur DNS.
Serveur DNS 2	Si Serveurs DNS de DHCP est défini sur Désactivé , entrez l'adresse IP du deuxième serveur DNS.
Paramètres IPv6	
IPv6	Activez ou désactivez la prise en charge de la connexion IPv6.
Source d'adresse IPv6	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. 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. Si la source d'adresse IP est définie sur Statique , entrez 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 AutoConfig , ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP. Si la source d'adresse IP est définie sur Statique , entrez l'adresse IP de la passerelle par défaut.
Adresse locale du lien IPv6	Il s'agit de l' adresse locale du lien IPv6 non modifiable de l'interface réseau iDRAC6.
Adresses 2 à 15 IPv6	Il s'agit des adresses IPv6 2 ... à IPv6 15 non modifiables de l'interface réseau iDRAC6.
Serveurs DNS de DHCPv6	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 , entrez l'adresse IP du premier serveur DNS.
Serveur DNS 2	Si Serveurs DNS de DHCP est défini sur Désactivé , entrez l'adresse IP du premier serveur DNS.

Configuration du média virtuel

Média virtuel

Utilisez les touches fléchées gauche et droite pour sélectionner **Autoconnecté**, **Connecté** ou **Déconnecté**.

- 1 Si vous sélectionnez **Connecté**, les périphériques de média virtuel sont connectés au bus USB, ce qui les rend disponibles lors des sessions de console virtuelle.
- 1 Si vous sélectionnez **Déconnecté**, les utilisateurs ne peuvent pas accéder aux périphériques de média virtuel lors des sessions de console virtuelle.
- 1 Si vous sélectionnez **Autoconnecté**, les périphériques de média virtuel sont automatiquement connectés au serveur au démarrage d'une session de média virtuel.

 **REMARQUE :** Pour utiliser un lecteur Flash USB avec la fonctionnalité Média virtuel, le **type d'émulation de lecteur Flash USB** doit être défini sur **Disque dur** dans l'utilitaire de configuration du BIOS. Accédez à l'utilitaire de configuration du BIOS en appuyant sur <F2> lors du démarrage du serveur. Si le **type d'émulation de lecteur Flash USB** est défini sur **Automatique**, le lecteur Flash apparaît sous forme de lecteur de disquette sur le système.

vFlash

Utilisez la flèche gauche et la flèche droite pour sélectionner **Activé** ou **Désactivé**.

- 1 **Activé** : vFlash est disponible pour la gestion des partitions.
- 1 **Désactivé** : vFlash n'est pas disponible pour la gestion des partitions.

 **PRÉCAUTIONS : vFlash ne peut pas être désactivé si une ou plusieurs partitions sont utilisées ou connectées.**

Initialiser vFlash

Choisissez cette option pour initialiser la carte vFlash. L'opération d'initialisation efface les données existantes sur la carte SD et toutes les partitions existantes sont supprimées. Vous ne pouvez pas exécuter l'opération d'initialisation si une ou plusieurs partitions sont utilisées ou connectées. Cette option est accessible uniquement si une carte d'une taille supérieure à 256 Mo est présente dans le logement de carte d'iDRAC Enterprise et si vFlash est activé.

Appuyez sur <Entrée> pour initialiser la carte SD vFlash.

L'opération d'initialisation peut échouer pour les raisons suivantes :

- 1 La carte SD n'est pas présente.
- 1 vFlash est actuellement utilisé par un autre processus.
- 1 vFlash n'est pas activé.
- 1 La carte SD est protégée contre l'écriture.
- 1 Une ou plusieurs partitions sont actuellement utilisées.
- 1 Une ou plusieurs partitions sont actuellement connectées.

Propriétés de vFlash

Appuyez sur <Entrée> pour afficher les propriétés suivantes de la carte SD vFlash :

- 1 **Nom** : affiche le nom de la carte SD vFlash insérée dans le logement de carte SD vFlash du serveur. S'il s'agit d'une carte SD Dell, la mention « Carte SD vFlash » apparaît. S'il s'agit d'une carte SD autre que Dell, la mention « Carte SD » apparaît.
- 1 **Taille** : affiche la taille de la carte SD vFlash en gigaoctets (Go).
- 1 **Espace disponible** : affiche l'espace inutilisé sur la carte SD vFlash en mégaoctets (Mo). Cet espace est disponible pour créer d'autres partitions sur la carte SD vFlash. Pour les cartes SD, la mention « 256 Mo » apparaît pour spécifier l'espace disponible.
- 1 **Protégé contre l'écriture** : indique si la carte SD vFlash est protégée ou non contre l'écriture.
- 1 **Intégrité** : affiche l'intégrité générale de la carte SD vFlash. Elle peut être :
 - o OK
 - o Avertissement
 - o Critique

Appuyez sur <Échap> pour quitter.

Carte à puce/SSO

Cette option configure les fonctionnalités **Connexion par carte à puce** et **Connexion directe**. Les options disponibles sont **Activé** et **Désactivé**.

 **REMARQUE** : Si vous activez la fonctionnalité **Connexion directe**, la fonctionnalité **Connexion par carte à puce** est désactivée.

Services système

Services système

Utilisez la flèche gauche et la flèche droite pour sélectionner **Activé** ou **Désactivé**. Si vous choisissez **Activé**, vous pouvez configurer certaines fonctionnalités iDRAC6 via Lifecycle Controller. Pour plus d'informations, consultez le *Guide d'utilisation de Lifecycle Controller*, disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

 **REMARQUE** : La modification de cette option redémarre le serveur lorsque vous utilisez **Enregistrer** et **Quitter** pour appliquer les nouveaux paramètres.

Annuler les services système

Utilisez les touches fléchées haut et bas pour sélectionner **Oui** ou **Non**.

Lorsque vous sélectionnez **Oui**, toutes les sessions de Lifecycle Controller 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 redémarre le serveur une fois que vous avez enregistré vos paramètres et quitté l'utilitaire de configuration iDRAC6.

Configuration de l'utilisateur LAN

L'utilisateur LAN est le compte administrateur iDRAC6, soit **root** par défaut. Appuyez sur <Entrée> pour afficher le sous-menu Configuration utilisateur LAN. Une fois la configuration de l'utilisateur LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

Tableau 18-2. Écran Configuration utilisateur LAN

Élément	Description
Découverte automatique	<p>La fonctionnalité Découverte automatique permet la découverte automatique de systèmes sans provisionnement sur le réseau ; elle permet en outre d'établir des références initiales <i>de manière sécurisée</i> afin que ces systèmes découverts puissent être gérés. Cette fonctionnalité permet à iDRAC6 de détecter le serveur d'approvisionnement. iDRAC6 et le serveur du service de provisionnement s'authentifient mutuellement. Le serveur d'approvisionnement 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 WSMAN avec iDRAC6 à l'aide des informations d'identification spécifiées dans le processus de détection et envoyer ensuite les instructions sécurisées à iDRAC6 afin de déployer un système d'exploitation à distance.</p> <p>Pour plus d'informations sur le déploiement d'un système d'exploitation à distance, consultez le <i>Guide d'utilisation de Dell Lifecycle Controller</i> disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.</p> <p>Exécutez les actions requises suivantes dans une session de l'utilitaire de configuration iDRAC6 <i>séparée avant d'établir manuellement la découverte automatique</i> :</p> <ul style="list-style-type: none">1 Activer le NIC (serveurs lames)1 Activer IPv4 (serveurs lames)1 Activer DHCP1 Obtenir le nom de domaine auprès de DHCP1 Désactiver le compte admin (compte n° 2)1 Obtenir l'adresse du serveur DNS auprès de DHCP1 Obtenir le nom de domaine DNS auprès de DHCP <p>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 définie sur Activé, iDRAC6 sur le système Dell est alors livré avec DHCP activé sans références par défaut pour l'ouverture de session à distance.</p>
Découverte automatique (suite...)	<p>Avant l'ajout de votre système Dell au réseau et l'utilisation de la fonctionnalité Découverte automatique, assurez-vous que :</p> <ul style="list-style-type: none">1 Le serveur DHCP (protocole de configuration dynamique de l'hôte)/le système de noms de domaine (DNS) sont configurés.1 Les services Web de provisionnement sont installés, configurés et enregistrés.
Serveur d'approvisionnement	<p>Ce champ est utilisé pour configurer le serveur d'approvisionnement. L'adresse du serveur d'approvisionnement peut être une combinaison d'adresses IPv4 ou de noms d'hôtes et ne doit pas excéder 255 caractères. Chaque adresse ou nom d'hôte doit être séparé par une virgule.</p> <p>Si vous avez activé la fonctionnalité Découverte automatique, les informations d'identification de l'utilisateur sont récupérées sur le serveur d'approvisionnement configuré pour permettre un provisionnement à distance ultérieur une fois le processus de découverte automatique correctement terminé.</p> <p>Pour plus d'informations, consultez le <i>Guide d'utilisation de Dell Lifecycle Controller</i> disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.</p>
Accès au compte	<p>Sélectionnez Activé pour activer le compte administrateur. Sélectionnez Désactivé pour désactiver le compte d'administrateur ou lorsque Découverte automatique est activé.</p>
Privilège LAN IPMI	<p>Choisissez entre Administrateur, Utilisateur, Opérateur et Aucun accès.</p>
Nom d'utilisateur de compte	<p>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.</p>
Entrer le mot de passe	<p>Entrez le nouveau mot de passe du compte administrateur. Les caractères ne sont pas renvoyés sur l'affichage lorsque vous les entrez.</p>
Confirmer le mot de passe	<p>Retapez le nouveau mot de passe du compte administrateur. Si les caractères que vous avez entrés ne correspondent pas à ceux que vous avez tapés dans le champ Entrer le mot de passe, un message s'affiche, et vous devez entrer à nouveau le mot de passe.</p>

Rétablir les paramètres par défaut

Utilisez l'élément de menu **Rétablir les paramètres par défaut** pour rétablir les paramètres d'usine de tous les éléments de la configuration iDRAC6. Cette opération peut être requise, par exemple, si vous avez oublié le mot de passe utilisateur d'administration ou si vous souhaitez reconfigurer iDRAC6 à partir des paramètres par défaut.

 **REMARQUE :** Dans la configuration par défaut, la mise en réseau iDRAC6 est désactivée. Vous ne pouvez pas reconfigurer iDRAC6 sur le réseau tant que vous n'avez pas activé le réseau iDRAC6 dans l'utilitaire de configuration iDRAC6.

Appuyez sur <Entrée> pour sélectionner l'élément. Le message d'avertissement suivant apparaît :

Resetting to factory defaults will restore remote Non-Volatile user settings. Continue
(La réinitialisation des paramètres d'usine va restaurer les paramètres utilisateur non volatiles à distance. Continuer)

< NO (Cancel) (NON (Annuler)) >

< YES (Continue)(OUI (Continuer)) >

Sélectionnez **OUI** et appuyez sur <Entrée> pour rétablir les paramètres par défaut d'iDRAC6.

L'un des messages d'erreur suivants s'affiche si cette opération échoue :

- 1 La commande reset n'a pas abouti. Veuillez réessayer ultérieurement ; iDRAC est occupé.
- 1 Échec de restauration des valeurs par défaut des paramètres : délai d'attente.
- 1 Impossible d'envoyer la commande reset. Veuillez réessayer ultérieurement ; iDRAC est occupé.

Menu Journal des événements système

Le menu **Journal des événements système** vous permet d'afficher les messages du journal des événements système (SEL) et d'effacer les messages du journal. Appuyez sur <Entrée> pour afficher le menu **Journal des événements système**. Le système compte les entrées de journal, puis affiche le nombre total d'enregistrements et le message le plus récent. Le journal SEL conserve un maximum de 512 messages.

Pour afficher les messages du journal SEL, sélectionnez **Afficher le journal des événements système** et appuyez sur <Entrée>. Pour naviguer :

- 1 Utilisez la flèche gauche pour accéder au message précédent (plus ancien) et la flèche droite pour accéder au message suivant (plus récent).
- 1 Entrez un numéro d'enregistrement spécifique pour atteindre cet enregistrement.

Appuyez sur <Échap> pour quitter le journal des événements système.

 **REMARQUE :** Vous pouvez uniquement effacer les messages du journal SEL dans l'utilitaire de configuration iDRAC6 ou dans l'interface Web iDRAC6.

Pour effacer les messages du journal SEL, sélectionnez **Effacer le journal des événements système** et appuyez sur <Entrée>.

Lorsque vous avez fini d'utiliser le menu Journal SEL, appuyez sur <Échap> pour revenir au menu précédent.

Sortie de l'utilitaire de configuration iDRAC6

Lorsque vous avez fini d'apporter des modifications à la configuration iDRAC6, appuyez sur la touche <Échap> pour afficher le menu Quitter.

- 1 Sélectionnez **Enregistrer les modifications et quitter** et appuyez sur <Entrée> pour conserver vos modifications. Si cette opération échoue, l'un des messages suivants s'affiche :
 - o iDRAC6 Communication Failure-Displayed if iDRAC is not accessible. (Échec de la communication iDRAC6 : s'affiche si iDRAC n'est pas accessible).
 - o Some of the settings cannot be applied-Displayed when few settings cannot be applied. (Certains des paramètres ne peuvent pas être appliqués : s'affiche lorsqu'un petit nombre de paramètres ne peut pas être appliqué).
- 1 Sélectionnez **Ignorer les modifications et quitter** et appuyez sur <Entrée> pour ignorer les modifications que vous avez apportées.
- 1 Sélectionnez **Retour au programme d'installation** et appuyez sur <Entrée> pour revenir dans l'utilitaire de configuration iDRAC6.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Récupération et dépannage du système géré

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers version 3.0 Guide d'utilisation

- [La sécurité d'abord : Pour vous et votre système](#)
- [Voyants inhérents aux problèmes](#)
- [Outils de résolution des problèmes](#)
- [Dépannage et questions les plus fréquentes](#)

Cette section explique comment effectuer les tâches relatives au diagnostic et au dépannage d'un système géré distant à l'aide des utilitaires iDRAC6. Elle contient les sous-sections suivantes :

- 1 Indications concernant les problèmes - vous aide à rechercher les messages et d'autres indications système en vue d'établir un diagnostic du problème
- 1 Outils de résolution des problèmes - décrit les outils iDRAC6 que vous pouvez utiliser pour dépanner votre système
- 1 Dépannage et questions les plus fréquentes - répond aux situations types que vous êtes susceptibles de rencontrer

La sécurité d'abord : Pour vous et votre système

Pour effectuer certaines procédures de cette section, vous devez utiliser le châssis, le système Dell PowerEdge ou d'autres modules matériels. N'essayez pas de réparer le matériel du système par vous-même. Tenez-vous en aux explications fournies dans ce guide et dans votre documentation système.

⚠ PRÉCAUTIONS : La plupart des réparations ne peuvent être effectuées que par un technicien de maintenance agréé. Vous êtes uniquement autorisé à effectuer les opérations de dépannage et les simples réparations conformément aux spécifications de votre documentation produit ou conformément aux instructions qui vous sont fournies en ligne, par téléphone et par l'équipe de support. Tout dommage causé par une réparation non autorisée par Dell est exclu de votre garantie. Consultez et respectez les consignes de sécurité fournies avec votre produit.

Voyants inhérents aux problèmes

Cette section décrit les indications concernant les problèmes susceptibles de se produire sur votre système.

Voyants LED

Le signalement initial de tout problème sur le système peut se faire via les LED présentes sur le châssis ou les composants installés dans le châssis. Les composants et modules suivants sont dotés de LED de condition :

- 1 Écran LCD du châssis
- 1 Serveurs
- 1 Ventilateurs
- 1 CMC
- 1 Modules d'E/S
- 1 Blocs d'alimentation

La LED unique sur l'écran LCD du châssis résume la condition de tous les composants du système. Une LED bleue unie sur l'écran LCD indique qu'aucune condition d'anomalie n'a été détectée sur le système. Une LED orange qui clignote sur l'écran LCD indique qu'une ou plusieurs conditions d'anomalie ont été détectées.

Si une LED orange clignote sur l'écran LCD du châssis, vous pouvez utiliser le menu d'écran LCD pour localiser le composant présentant une anomalie. Consultez le *Guide d'utilisation du micrologiciel Dell Chassis Management Controller* pour obtenir de l'aide concernant l'utilisation de l'écran LCD.

[Tableau 19-1](#) décrit les significations de la LED sur le système Dell PowerEdge :

Tableau 19-1. Voyants LED du serveur lame

Voyant LED	Signification
vert uni (<i>uniquement pour le bouton d'alimentation</i>)	Le serveur est sous tension. L'absence de LED verte signifie que le serveur n'est pas sous tension.
bleu uni	iDRAC6 est intègre.
orange clignotant	iDRAC6 a détecté une condition d'anomalie ou s'apprête à mettre à jour le micrologiciel.
bleu clignotant	Un utilisateur a activé la référence de l'indicateur d'emplacement pour ce serveur.

Voyants inhérents aux problèmes du matériel

Les indications de problèmes du matériel sur un module sont les suivantes :

- 1 Échec de la mise sous tension
- 1 Ventilateurs bruyants
- 1 Perte de connectivité réseau
- 1 Alertes de batterie, de température, de tension ou de capteur de contrôle de l'alimentation
- 1 Pannes de disque dur
- 1 Panne du média USB
- 1 Endommagement physique provoqué par une chute, de l'eau ou toute autre contrainte externe

Lorsque ces types de problème se produisent, examinez le dommage causé, puis essayez de corriger le problème grâce aux stratégies suivantes :

- 1 Repositionnez le module et redémarrez-le
- 1 Essayez d'insérer le module dans une baie différente du châssis
- 1 Essayez de remplacer les disques durs ou les clés USB
- 1 Reconnectez ou remplacez les câbles d'alimentation et réseau

Si ces étapes ne permettent pas de corriger le problème, consultez le *Manuel du propriétaire du matériel* pour obtenir des informations de dépannage spécifiques concernant le périphérique matériel.

Autres voyants inhérents aux problèmes

Tableau 19-2. Voyants inhérents aux problèmes

Recherchez :	Action :
Des messages d'alerte du logiciel Systems Management Software	Consultez la documentation du logiciel Systems Management Software.
Messages dans le journal des événements système	Consultez Vérification du journal des événements système (SEL) .
Messages dans les codes POST de démarrage	Consultez Vérification des codes POST .
Messages sur l'écran de la dernière panne	Consultez Affichage de l'écran de la dernière panne système .
Messages d'alerte sur l'écran de condition du serveur sur l'écran LCD	Consultez Vérification des messages d'erreur dans l'écran de condition du serveur .
Messages dans le journal iDRAC6	Consultez Affichage du journal iDRAC6 .

Outils de résolution des problèmes

Cette section décrit les utilitaires iDRAC6 que vous pouvez utiliser pour diagnostiquer des problèmes sur votre système, notamment lorsque vous essayez de les résoudre à distance.

- 1 Vérification de l'intégrité du système
- 1 Vérification des messages d'erreur dans le journal des événements système
- 1 Vérification des codes POST
- 1 Affichage de l'écran de la dernière panne
- 1 Visualisation des dernières séquences d'amorçage
- 1 Vérification des messages d'erreur dans l'écran de condition du serveur sur l'écran LCD
- 1 Affichage du journal iDRAC6
- 1 Affichage des informations sur le système
- 1 Identification du serveur géré dans le châssis
- 1 Utilisation de la console de diagnostics
- 1 Gestion de l'alimentation d'un système distant

Vérification de l'intégrité du système

Lorsque vous ouvrez une session sur l'interface Web iDRAC6, l'écran **Résumé du système** affiche l'intégrité des composants système. [Tableau 19-3](#) décrit la signification des voyants d'intégrité du système.

Tableau 19-3. Voyants d'intégrité du serveur

--	--

Voyant	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.

Cliquez sur un composant quelconque de la section **Intégrité du serveur** pour afficher les informations sur le composant. Les lectures de capteur s'affichent pour les batteries, les températures, les tensions et le contrôle de l'alimentation, vous aidant ainsi à diagnostiquer certains types de problèmes. Les écrans d'informations iDRAC6 et CMC contiennent des informations utiles sur la configuration et la condition actuelles.

Vérification du journal des événements système (SEL)

L'écran **Journal SEL** affiche les messages des événements qui se produisent sur le serveur géré.

Pour afficher le **journal des événements système**, suivez les étapes suivantes :

1. Cliquez sur **Système**, puis sur l'onglet **Journaux**.
2. Cliquez sur **Journal des événements système** pour afficher l'écran **Journal des événements système**.
L'écran **Journal des événements système** affiche un voyant d'intégrité système (consultez [Tableau 19-3](#)), un horodateur et une description de l'événement.
3. Cliquez sur le bouton **Journal des événements système** approprié pour continuer (consultez [Tableau 19-4](#)).

Tableau 19-4. Boutons du journal SEL

Bouton	Action
Imprimer	Imprime le journal SEL dans l'ordre de tri qui apparaît dans la fenêtre .
Effacer le journal	Efface le journal SEL. REMARQUE : Le bouton Effacer le journal n'apparaît que si vous disposez de l'autorisation Effacer les journaux .
Enregistrer sous	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer le journal SEL dans le répertoire de votre choix. REMARQUE : Si vous utilisez Internet Explorer et rencontrez un problème lors de l'enregistrement, téléchargez Cumulative Security Update for Internet Explorer à partir du site Web du support de Microsoft à l'adresse support.microsoft.com . REMARQUE : Lorsque vous utilisez Internet Explorer, si vous n'êtes pas en mesure d'enregistrer le journal SEL à l'aide d' Enregistrer sous , cela peut être dû à un paramètre du navigateur. Pour y remédier : <ol style="list-style-type: none">1. Dans Internet Explorer, accédez à Outils→Options Internet→Sécurité et sélectionnez la zone dans laquelle vous essayez d'effectuer un téléchargement. Par exemple, si le périphérique iDRAC se trouve sur votre Intranet local, sélectionnez Intranet local et cliquez sur Personnaliser le niveau...2. Dans la fenêtre Paramètres de sécurité, sous Téléchargements, vérifiez que les options suivantes sont activées :<ul style="list-style-type: none">o Demander confirmation pour les téléchargements de fichierso Téléchargement de fichiers PRÉCAUTIONS : Pour vous assurer que l'ordinateur utilisé pour accéder à iDRAC est sûr, sous Divers , l'option Lancement des applications et des fichiers non sûrs ne doit pas être activée .
Actualiser	Recharge l'écran du journal SEL.

Vérification des codes POST

L'écran **Codes POST** affiche le dernier code POST du système avant le démarrage du système d'exploitation. Les codes POST sont les indicateurs de progression du BIOS du système, indiquant les diverses étapes de la séquence d'amorçage suite à une mise sous tension et vous permettent de diagnostiquer les erreurs de démarrage du système.

 **REMARQUE :** Affichez le texte pour rechercher les numéros de message du code POST sur l'écran LCD ou dans le *Manuel du propriétaire du matériel*.

Pour afficher les codes POST, suivez les étapes suivantes :

1. Cliquez sur **Système**, cliquez sur l'onglet **Journaux**, puis sur **Code POST**.

L'écran **Code POST** affiche un voyant d'intégrité système (consultez [Tableau 19-3](#)), un code hexadécimal et une description du code.

2. Cliquez sur le bouton approprié de l'écran **Code POST** pour continuer (consultez [Tableau 19-5](#)).

Tableau 19-5. Boutons du code POST

Bouton	Action
Imprimer	Imprime l'écran Code POST.
Actualiser	Recharge l'écran Code POST.

Affichage de l'écran de la dernière panne système

REMARQUE : La fonctionnalité Écran de la dernière panne doit être configurée dans Server Administrator et dans l'interface Web iDRAC6. Consultez [Configuration du serveur géré pour la capture de l'écran de la dernière panne](#) pour obtenir des instructions sur la configuration de cette fonctionnalité.

L'**écran de la dernière panne** affiche l'écran de la panne la plus récente, qui comprend des informations sur les événements qui se sont produits avant la panne du système. L'image de la dernière panne du système est enregistrée dans le magasin permanent d'iDRAC6 et est accessible à distance.

Pour afficher l'**écran de la dernière panne**, suivez les étapes suivantes :

1. Cliquez sur **Système**, cliquez sur l'onglet **Journaux**, puis sur **Écran de la dernière panne**.

L'**écran de la dernière panne** inclut les boutons présentés dans [Tableau 19-6](#) :

REMARQUE : Les boutons **Enregistrer** et **Supprimer** n'apparaissent pas en l'absence d'écran de panne enregistré.

Tableau 19-6. Boutons de l'écran de la dernière panne

Bouton	Action
Imprimer	Imprime l'écran de la dernière panne.
Enregistrer	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer l'écran de la dernière panne dans le répertoire de votre choix.
Supprimer	Supprime l'écran de la dernière panne.
Actualiser	Recharge l'écran de la dernière panne.

REMARQUE : En raison des fluctuations dans l'horloge de récupération automatique, l'**écran de la dernière panne** peut ne pas être capturé lorsque l'horloge de réinitialisation du système est configurée avec une valeur trop élevée. Le paramètre par défaut est 480 secondes. Utilisez Server Administrator ou IT Assistant pour définir l'horloge de réinitialisation du système sur 60 secondes et s'assurer que la fonctionnalité **Écran de la dernière panne** fonctionne correctement. Pour plus d'informations, consultez [Configuration du serveur géré pour la capture de l'écran de la dernière panne](#).

Visualisation des dernières séquences d'amorçage

Si vous rencontrez des problèmes lors de l'amorçage, vous pouvez visualiser à l'écran les événements qui se sont produits au cours des trois dernières séquences d'amorçage dans l'écran **Capture au démarrage**. Les écrans d'amorçage sont lus à la vitesse de 1 trame par seconde. iDRAC6 enregistre 50 trames au cours du démarrage.

[Tableau 19-7](#) répertorie les actions de contrôle disponibles.

REMARQUE : Vous devez posséder des droits d'administrateur pour lire les séquences de capture au démarrage.

Tableau 19-7. Options de capture au démarrage

Bouton/Option	Description
Sélectionner la séquence d'amorçage	Vous permet de sélectionner la séquence d'amorçage à charger et à lire. <ol style="list-style-type: none"> 1 Capture au démarrage 1 : charge la dernière séquence d'amorçage. 1 Capture au démarrage 2 : charge la (deuxième plus récente) séquence d'amorçage qui s'est produite avant la capture au démarrage 1. 1 Capture au démarrage 3 : charge la (troisième plus récente) séquence d'amorçage qui s'est produite avant la capture au démarrage 2.
Enregistrer sous	Crée un fichier .zip compressé contenant toutes les images de capture au démarrage de la séquence courante. L'utilisateur doit posséder des droits d'administrateur pour effectuer cette action.
Écran précédent	Vous ramène à l'écran précédent, le cas échéant, dans la console de relecture.
Lire	Lance le scénario depuis l'écran actuel dans la console de relecture.

Pause	Interrompt temporairement le scénario sur l'écran actuel affiché dans la console de relecture.
Arrêter	Arrête le scénario et charge le premier écran de cette séquence d'amorçage.
Écran suivant	Vous amène à l'écran suivant, le cas échéant, dans la console de relecture.
Imprimer	Imprime l'image de capture au démarrage qui apparaît à l'écran.
Actualiser	Recharge l'écran Capture au démarrage.

Vérification des messages d'erreur dans l'écran de condition du serveur

Lorsqu'une LED orange clignote, et qu'une erreur s'est produite sur un serveur particulier, l'écran de condition du serveur principal sur l'écran LCD met en surbrillance le serveur affecté en orange. Utilisez les boutons de navigation de l'écran LCD pour mettre en surbrillance le serveur affecté, puis cliquez sur le bouton central. Les messages d'erreur et d'avertissement s'affichent sur la deuxième ligne. Le tableau suivant répertorie tous les messages d'erreur et leur gravité.

Tableau 19-8. Écran Condition du serveur

Gravité	Message	Cause
Avertissement	System Board Ambient Temp: Temperature sensor for System Board, warning event (Temp. ambiante de la carte système : capteur de température de la carte système, événement d'avertissement)	La température ambiante du serveur a franchi un seuil d'avertissement
Critique	System Board Ambient Temp: Temperature sensor for System Board, failure event (Temp. ambiante de la carte système : capteur de température de la carte système, événement de panne)	La température ambiante du serveur a franchi un seuil de panne
Critique	System Board CMOS Battery: Battery sensor for System Board, failed was asserted (Batterie CMOS de la carte système : capteur de batterie de la carte système ; la panne a été confirmée)	La batterie CMOS est absente ou sa tension est nulle
Avertissement	System Board System Level: Current sensor for System Board, warning event (Niveau système de la carte système : capteur de courant de la carte système, événement d'avertissement)	Le courant a franchi un seuil d'avertissement
Critique	System Board System Level: Current sensor for System Board, failure event (Niveau système de la carte système : capteur de courant de la carte système, événement de panne)	Le courant a franchi un seuil de panne
Critique	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (UC<numéro> <nom du capteur de tension> : capteur de tension de l'UC<numéro>, l'état confirmé a été confirmé)	Tension hors plage
Critique	System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted (Carte système <nom du capteur de tension> : capteur de tension de la carte système, l'état confirmé a été confirmé)	Tension hors plage
Critique	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (UC<numéro> <nom du capteur de tension> : capteur de tension de l'UC<numéro>, l'état confirmé a été confirmé)	Tension hors plage
Critique	CPU<number> Status: Processor sensor for CPU<number>, IERR was asserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, l'IERR a été confirmé)	Panne de l'UC
Critique	CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, le dépassement thermique a été confirmé)	UC surchauffée
Critique	CPU<number> Status: Processor sensor for CPU<number>, configuration error was asserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, l'erreur de configuration a été confirmée)	Type de processeur incorrect ou dans un emplacement erroné
Critique	CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted (Condition de l'UC<numéro> : capteur du processeur de l'UC<numéro>, la confirmation de la présence a été annulée)	L'UC requise est manquante ou est absente
Critique	System Board Video Riser: Module sensor for System Board, device removed was asserted (Carte de montage vidéo de la carte système : capteur de module de la carte système, le périphérique retiré a été confirmé)	Le module requis a été retiré
Critique	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted (Condition de la carte Mezz B<numéro de logement> : capteur de carte d'extension de la carte Mezz B<numéro de logement>, l'erreur d'installation a été confirmée)	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted (Condition de la carte Mezz C<numéro de logement> : capteur de carte d'extension de la carte Mezz C<numéro de logement>, l'erreur d'installation a été confirmée)	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed (Lecteur de fond de panier <numéro> : capteur de logement du lecteur de fond de panier, lecteur retiré)	Le lecteur de stockage a été retiré

Critique	Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted (Lecteur de fond de panier <numéro> : capteur de logement du lecteur de fond de panier, la panne du lecteur a été confirmée)	Le lecteur de stockage a échoué
Critique	System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted (Prévention de défaillance PFault de la carte système : capteur de tension de la carte système, l'état confirmé a été confirmé)	Cet événement est généré lorsque les tensions de la carte système ne sont pas aux niveaux normaux
Critique	System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, le délai expiré a été confirmé)	Le registre d'horloge de la surveillance iDRAC6 a expiré et aucune action n'est définie
Critique	System Board OS Watchdog: Watchdog sensor for System Board, reboot was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, le redémarrage a été confirmé)	La surveillance iDRAC6 a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte) et que l'action est définie sur redémarrage.
Critique	System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, la mise hors tension a été confirmée)	La surveillance iDRAC6 a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte) et que l'action est définie sur mise hors tension
Critique	System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted (Surveillance du SE de la carte système : capteur de surveillance de la carte système, le cycle d'alimentation a été confirmé)	La surveillance iDRAC6 a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte) et que l'action est définie sur cycle d'alimentation
Critique	System Board SEL: Event Log sensor for System Board, log full was asserted (Journal SEL de la carte système : capteur du journal des événements de la carte système, la plénitude du journal a été confirmée)	Le périphérique du journal SEL détecte qu'une seule entrée peut être ajoutée au journal SEL avant qu'il ne soit plein
Avertissement	ECC Corr Err: Memory sensor, correctable ECC (<DIMM Location>) was asserted (Err ECC corr : capteur de mémoire, l'ECC corrigéable (<emplacement de la barrette DIMM>) a été confirmée)	Les erreurs ECC corrigéables ont atteint un taux critique
Critique	ECC Uncorr Err: Memory sensor, uncorrectable ECC(<DIMM Location>) was asserted (Err ECC non corr : capteur de mémoire, l'ECC non corrigéable (<emplacement de la barrette DIMM>) a été confirmée)	Une erreur ECC non corrigéable a été détectée
Critique	I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted (Contrôle du canal d'E/S : capteur d'événement critique, le NMI du contrôle du canal d'E/S a été confirmé)	Une interruption critique est générée dans le canal d'E/S
Critique	PCI Parity Err: Critical Event sensor, PCI PERR was asserted (Err de parité PCI : capteur d'événement critique, le PERR PCI a été confirmé)	Une erreur de parité a été détectée sur le bus PCI
Critique	PCI System Err: Critical Event sensor, PCI SERR (<Slot number or PCI Device ID>) was asserted (Erreur du système PCI : capteur d'événement critique, le SERR PCI (<numéro de logement ou réf. périphérique PCI>) a été confirmé)	Erreur PCI détectée par le périphérique
Critique	SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted (Journal SBE désactivé : capteur du journal des événements, la journalisation des erreurs mémoire corrigéables a été confirmée)	La journalisation des erreurs portant sur un seul bit est désactivée lorsqu'un nombre trop élevé de SBE est journalisé
Critique	Logging Disabled: Event Log sensor, all event logging disabled was asserted (Journalisation désactivée : capteur du journal des événements, la journalisation systématique des événements désactivée a été confirmée)	La journalisation de toutes les erreurs est désactivée
Irrécupérable	CPU Protocol Err: Processorsensor, transition to non-recoverable was asserted (Err protocole de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée)	Le protocole du processeur est passé à l'état irrécupérable
Irrécupérable	CPU Bus PERR: Processor sensor, transition to non-recoverable was asserted (PERR du bus de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée)	Le PERR du bus du processeur est passé à l'état irrécupérable
Irrécupérable	CPU Init Err: Processor sensor, transition to non-recoverable was asserted (Err d'init de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée)	L'initialisation du processeur est passée à l'état irrécupérable
Irrécupérable	CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted (Machine Check de l'UC : capteur du processeur, la transition à irrécupérable a été confirmée)	Le Machine Check du processeur est passé à l'état irrécupérable
Critique	Memory Spared: Memory sensor, redundancy lost(<DIMM Location>) was asserted (Mémoire de secours : capteur de mémoire, la redondance perdue (<emplacement de la barrette DIMM>) a été confirmée)	La mémoire de secours n'est plus redondante
Critique	Memory Mirrored: Memory sensor, redundancy lost(<DIMM Location>) was asserted (Mémoire en miroir : capteur de mémoire, la redondance perdue (<emplacement de la barrette DIMM>) a été confirmée)	La mémoire en miroir n'est plus redondante
Critique	Memory RAID: Memory sensor, redundancy lost(<DIMM Location>) was asserted (Mémoire RAID : capteur de mémoire, la redondance perdue (<emplacement de la barrette DIMM>) a été confirmée)	La mémoire RAID n'est plus redondante
Avertissement	Memory Added: Memory sensor, presence (<DIMM Location>) was deasserted (Mémoire ajoutée : capteur de mémoire, la confirmation de la présence (<emplacement de la barrette DIMM>) a été annulée)	Le module de mémoire ajoutée a été retiré
Avertissement	Memory Removed: Memory sensor, presence (<DIMM Location>) was deasserted (Mémoire retirée : capteur de mémoire, la confirmation de la présence (<emplacement de la barrette DIMM>) a été annulée)	Le module de mémoire a été retiré

Critique	Memory Cfg Err: Memory sensor, configuration error(<DIMM Location>) was asserted (Err config mémoire : capteur de mémoire, l'erreur de configuration (<emplacement de la barrette DIMM>) a été confirmée)	La configuration de la mémoire est incorrecte pour le système
Avertissement	Mem Redun Gain: Memory sensor, redundancy degraded(<DIMM Location>) was asserted (Gain redon mém : capteur de mémoire, la redondance dégradée (<emplacement de la barrette DIMM>) a été confirmée)	La redondance de la mémoire est rétrogradée, mais n'est pas perdue
Critique	PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted (Err irrécupérable PCIE : capteur d'événement critique, l'erreur irrécupérable du bus a été confirmée)	Une erreur irrécupérable a été détectée sur le bus PCIE
Critique	Chipset Err: Critical Event sensor, PCI PERR was asserted (Err jeu de puces : capteur d'événement critique, le PERR PCI a été confirmé)	Une erreur de puce a été détectée
Avertissement	Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location>) was asserted (Avertissement ECC mém : capteur de mémoire, la transition de OK à non critique (<emplacement de la barrette DIMM>) a été confirmée)	Les erreurs corrigées de l'ECC ont dépassé le taux normal
Critique	Mem ECC Warning: Memory sensor, transition to critical from less severe (<DIMM Location>) was asserted (Avertissement ECC mém : capteur de mémoire, la transition de moins grave à critique (<emplacement de la barrette DIMM>) a été confirmée)	Les erreurs ECC corrigées ont atteint un taux critique
Critique	POST Err: POST sensor, Nomemory installed (Err POST : capteur POST, mémoire non installée)	Mémoire non détectée sur la carte
Critique	POST Err: POST sensor, Memory configuration error (Err POST : capteur POST, erreur de configuration de la mémoire)	Mémoire détectée mais non configurable
Critique	POST Err: POST sensor, Unusable memory error (Err POST : capteur POST, erreur de mémoire inutilisable)	Mémoire configurée mais inutilisable
Critique	POST Err: POST sensor, ShadowBIOS failed (Err POST : capteur POST, le BIOS en double a échoué)	Panne du BIOS en double système
Critique	POST Err: POST sensor, CMOSfailed (Err POST : capteur POST, le CMOS a échoué)	Panne du CMOS
Critique	POST Err: POST sensor, DMAcontroller failed (Err POST : capteur POST, le contrôleur DMA a échoué)	Panne du contrôleur DMA
Critique	POST Err: POST sensor, Interrupt controller failed (Err POST : capteur POST, le contrôleur d'interruptions a échoué)	Panne du contrôleur d'interruptions
Critique	POST Err: POST sensor, Timerrefresh failed (Err POST : capteur POST, l'actualisation du temporisateur a échoué)	Panne d'actualisation du temporisateur
Critique	POST Err: POST sensor, Programmable interval timererror (Err POST : capteur POST, erreur du temporisateur d'intervalle programmable)	Erreur du temporisateur d'intervalle programmable
Critique	POST Err: POST sensor, Parityerror (Err POST : capteur POST, erreur de parité)	Erreur de parité
Critique	POST Err: POST sensor, SIOfailed (Err POST : capteur POST, le SIO a échoué)	Panne du SIO
Critique	POST Err: POST sensor, Keyboard controller failed (Err POST : capteur POST, le contrôleur du clavier a échoué)	Panne du contrôleur du clavier
Critique	POST Err: POST sensor, Systemmanagement interrupt initialization failed (Err POST : capteur POST, l'initialisation de System Management Interrupt a échoué)	Panne d'initialisation de System Management Interrupt
Critique	POST Err: POST sensor, BIOSshutdown test failed (Err POST : capteur POST, le test d'arrêt du BIOS a échoué)	Panne du test d'arrêt du BIOS
Critique	POST Err: POST sensor, BIOSPOST memory test failed (Err POST : capteur POST, le test de mémoire POST du BIOS a échoué)	Panne du test mémoire du POST du BIOS
Critique	POST Err: POST sensor, Dellremote access controller configuration failed (Err POST : capteur POST, la configuration du contrôleur Dell Remote Access Controller a échoué)	Panne de la configuration du contrôleur Dell Remote Access Controller
Critique	POST Err: POST sensor, CPUconfiguration failed (Err POST : capteur POST, la configuration de l'UC a échoué)	Panne de configuration de l'UC
Critique	POST Err: POST sensor, Incorrect memory configuration (Err POST : capteur POST, configuration de la mémoire incorrecte)	Configuration de la mémoire incorrecte
Critique	POST Err: POST sensor, POSTfailure (Err POST : capteur POST, panne du POST)	Panne générale après la vidéo
Critique	Hdwar version err: Version Change sensor, hardware incompatibility was asserted (Err de version de matériel : capteur de changement de version, l'incompatibilité du matériel a été confirmée)	Un matériel incompatible a été détecté
Critique	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted (Err de version de matériel : capteur de changement de version, l'incompatibilité du matériel (micrologiciel BMC) a été confirmée)	Le matériel est incompatible avec le micrologiciel
Critique	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted (Err de version de matériel : capteur de changement de version, l'incompatibilité du matériel (micrologiciel BMC et non correspondance de l'UC) a été confirmée)	L'UC et le micrologiciel ne sont pas compatibles
Critique	Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted (Surchauffe de mém : capteur de mémoire, l'ECC corrigible (<emplacement de la barrette DIMM>) a été confirmé)	Le module de mémoire est en surchauffe
Critique	Mem Fatal SB CRC: Memory sensor, uncorrectable ECC was asserted (CRC SB irrécupérable de mém : capteur de mémoire, l'ECC non corrigible a	Panne de mémoire Southbridge

	été confirmé)	
Critique	Mem Fatal NB CRC: Memory sensor, uncorrectable ECC was asserted (CRC NB irrécupérable de mém : capteur de mémoire, l'ECC non corrigé a été confirmé)	Panne de mémoire Northbridge
Critique	WatchDog Timer: Watchdog sensor, reboot was asserted (Registre d'horloge de la surveillance : capteur de la surveillance, le redémarrage a été confirmé)	Le registre d'horloge de la surveillance a provoqué le redémarrage du système
Critique	WatchDog Timer: Watchdog sensor, timer expired was asserted (Registre d'horloge de la surveillance : capteur de la surveillance, le délai expiré a été confirmé)	Le registre d'horloge de la surveillance a expiré, mais aucune action n'a été prise
Avertissement	Link Tuning: Version Change sensor, successful software or F/W change was deasserted (Réglage de liaison : capteur de changement de version, la confirmation du changement réussi de logiciel ou de micrologiciel a été annulée)	La mise à jour du paramètre de réglage de liaison pour un fonctionnement NIC correct a échoué
Avertissement	Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted (Réglage de liaison : capteur de changement de version, la confirmation du changement réussi du matériel <numéro de logement du périphérique> a été annulée)	La mise à jour du paramètre de réglage de liaison pour un fonctionnement NIC correct a échoué
Critique	LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Fonction #) was asserted (Rég liaison/FlexAddress : capteur de réglage de liaison, l'échec de programmation de l'adresse MAC virtuelle (Bus # Périphérique # Fonction #) a été confirmé)	FlexAddress n'a pas pu être programmée pour ce périphérique
Critique	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) was asserted (Rég liaison/FlexAddress : capteur de réglage de liaison, l'échec de la prise en charge du réglage de liaison ou de l'adresse flex (Mezz <emplacement>) par la mémoire morte en option du périphérique a été confirmé)	La mémoire morte en option ne prend pas en charge FlexAddress ou le réglage de liaison
Critique	LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted (Rég liaison/FlexAddress : capteur de réglage de liaison, l'échec de l'obtention des données de réglage de liaison ou d'adresse flex de BMC/iDRAC6 a été confirmé)	Échec de l'obtention des informations de réglage de liaison ou de FlexAddress de BMC/iDRAC6
Critique	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or FlexAddress (Mezz XX) was asserted (Rég liaison/FlexAddress : capteur de réglage de liaison, l'échec de la prise en charge du réglage de liaison ou de FlexAddress (Mezz XX) par la mémoire morte en option du périphérique a été confirmé)	Cet événement est généré lorsque la mémoire morte en option du périphérique PCI pour un NIC ne prend pas en charge le réglage de liaison ou la fonctionnalité d'adressage Flex
Critique	LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted (Rég liaison/FlexAddress : capteur de réglage de liaison, l'échec de la programmation de l'adresse MAC virtuelle (<emplacement>) a été confirmé)	Cet événement est généré lorsque le BIOS ne parvient pas à programmer l'adresse MAC virtuelle sur le périphérique NIC donné
Critique	I/O Fatal Err: Fatal IO Group sensor, fatal IO error (<location>) (Err irrécupérable E/S : capteur de groupe d'E/S irrécupérable, erreur d'E/S irrécupérable (<emplacement>))	Cet événement est généré en association avec un IERR d'UC et indique le périphérique qui en est la cause
Avertissement	PCIe NonFatal Er: Non Fatal I/O Group sensor, PCIe error (<location>) (Er non irrécupérable PCIe : capteur de groupe d'E/S non irrécupérable, erreur PCIe (<emplacement>))	Cet événement est généré en association avec un IERR d'UC

Affichage du journal iDRAC6

Le journal iDRAC6 est un journal permanent conservé dans le micrologiciel iDRAC6. Le journal contient une liste des actions d'utilisateur (ouverture, fermeture de sessions et modifications des règles de sécurité, par exemple) et des alertes envoyées par iDRAC6. Ce journal est effacé après une mise à jour du micrologiciel iDRAC6.

Tandis que le journal des événements système (SEL) contient des enregistrements d'événements qui se produisent dans le serveur géré, le journal iDRAC6 contient des enregistrements d'événements qui se produisent dans iDRAC6.

Pour accéder au journal iDRAC6, suivez les étapes suivantes :

- 1 Cliquez sur **Système** → **Accès à distance** → **iDRAC6** → **Journaux**. L'écran Journal iDRAC6 apparaît. Cet écran contient les informations énoncées dans [Tableau 19-9](#).

Tableau 19-9. Informations du journal iDRAC6

Champ	Description
Date/Heure	Date et heure (par exemple, Dec 19 16:55:47). iDRAC6 définit son horloge à partir de celle du serveur géré lors de l'initialisation d'iDRAC6. Si le serveur géré est éteint au démarrage d'iDRAC6, iDRAC6 définit alors son horloge depuis le CMC dans le châssis dans lequel réside la lame. REMARQUE : Étant donné que la source d'heure pour iDRAC6 est différente en fonction de l'état de l'alimentation du serveur géré (au moment de l'initialisation d'iDRAC6), l'heure du serveur géré doit être définie pour correspondre à celle du CMC. Si l'heure du système et celle du CMC ne correspondent pas, les heures incohérentes peuvent être signalées dans les journaux d'iDRAC6 après les événements liés à l'initialisation d'iDRAC6.
Source	Interface qui a provoqué l'événement.

Description	Description brève de l'événement et nom de l'utilisateur qui s'est connecté à iDRAC6.
--------------------	---

Utilisation des boutons du journal iDRAC6

L'écran **Journal** iDRAC6 intègre les boutons suivants (consultez [Tableau 19-10](#)).

Tableau 19-10. Boutons du journal iDRAC6

Bouton	Action
Imprimer	Imprime l'écran Journal iDRAC6.
Effacer le journal	Efface les entrées du journal iDRAC6. REMARQUE : Le bouton Effacer le journal n'apparaît que si vous disposez de l'autorisation Effacer les journaux .
Enregistrer sous	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer le journal iDRAC6 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 l'écran Journal iDRAC6.

Affichage des informations système

L'écran **Détails du système** affiche des informations sur les composants système suivants :

- 1 Enceinte principale du système
- 1 Integrated Dell Remote Access Controller 6 - Enterprise

Pour accéder aux informations sur le système, cliquez sur **Système** → **Propriétés** → **Détails du système**.

Consultez la section « [Récupération et dépannage du système géré](#) » pour des informations sur le résumé du système, l'enceinte principale du système et iDRAC6.

Identification du serveur géré dans le châssis

Le châssis Dell PowerEdge M1000e contient jusqu'à seize serveurs. Pour rechercher un serveur spécifique dans le châssis, vous pouvez utiliser l'interface Web iDRAC6 pour activer une LED bleue qui clignote sur le serveur. Lorsque vous activez la LED, vous pouvez spécifier le nombre de secondes au cours desquelles vous souhaitez que la LED clignote afin de vous assurer que vous pouvez atteindre le châssis alors que la LED clignote toujours. Si vous entrez 0, la LED clignote tant que vous ne l'avez pas désactivée.

Pour identifier le serveur :

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6 → **Dépannage**.
2. Dans l'écran **Identifier**, sélectionnez **Identifier le serveur**.
3. Dans le champ **Délai d'attente d'identification du serveur**, entrez le nombre de secondes pendant lesquelles la LED doit clignoter. Entrez 0 si vous souhaitez que la LED clignote jusqu'à ce que vous la désactiviez.
4. Cliquez sur **Appliquer**.

Une LED bleue présente sur le serveur clignote pendant le nombre de secondes que vous avez spécifié.

Si vous avez entré 0 pour laisser la LED clignoter, suivez ces étapes pour la désactiver :

1. Cliquez sur **Système** → **Accès à distance** → iDRAC6 → **Dépannage**.
2. Dans l'écran **Identifier**, désélectionnez **Identifier le serveur**.
3. Cliquez sur **Appliquer**.

Utilisation de la console de diagnostics

iDRAC6 fournit un jeu standard d'outils de diagnostic réseau (consultez [Tableau 19-11](#)) 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.

Cliquez sur **Réinitialiser iDRAC6** pour réinitialiser iDRAC. Une opération de démarrage normale est effectuée sur iDRAC.

Pour accéder à l'écran **Console de diagnostics**, suivez les étapes suivantes :

1. Cliquez sur **Système** → **iDRAC6** → **Dépannage**.
2. Sélectionnez l'onglet **Console de diagnostics**.

[Tableau 19-11](#) décrit les commandes qui peuvent être entrées sur l'écran **Console de diagnostics**. Entrez une commande et cliquez sur **Envoyer**. Les résultats du débogage apparaissent dans l'écran **Console de diagnostics**.

Cliquez sur le bouton **Effacer** pour effacer les résultats affichés par la commande précédente.

Pour actualiser l'écran **Console de diagnostics**, cliquez sur **Actualiser**.

Tableau 19-11. Commandes de diagnostic

Commande	Description
arp	Affiche le contenu de la table du protocole de résolution d'adresses (ARP). Les entrées ARP ne peuvent être ni ajoutées, ni supprimées.
ifconfig	Affiche le contenu de la table d'interface réseau.
netstat	Imprime le contenu de la table de routage.
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. Il faut saisir une adresse IP de destination dans le champ à droite de cette option. Un paquet d'écho du protocole de contrôle des messages sur Internet (ICMP) est envoyé à l'adresse IP de destination en fonction du contenu actuel de la table de routage.
ping6 <adresse IPv6>	Vérifie que l'adresse IPv6 de destination est accessible à partir d'iDRAC6 avec le contenu actuel de la table de routage. Il faut saisir une adresse IPv6 de destination dans le champ à droite de cette option. Un paquet d'écho ICMP (protocole de contrôle des messages sur Internet) est envoyé à l'adresse IPv6 de destination en fonction du contenu actuel de la table de routage.
tracert <adresse IP>	Sert à déterminer le chemin emprunté par des paquets sur un réseau IP.
tracert6 <adresse IPv6>	Sert à déterminer le chemin emprunté par des paquets sur un réseau IPv6.
gettracelog	Affiche le journal de suivi d'iDRAC6. Pour plus d'informations, consultez gettracelog dans le <i>Guide de référence de l'administrateur d'iDRAC6</i> disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals .

Gestion de l'alimentation d'un système distant

iDRAC6 vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance sur un serveur géré. Utilisez l'écran **Gestion de l'alimentation** pour réaliser un arrêt méthodique du système d'exploitation lors des redémarrages et des mises sous tension et hors tension.

 **REMARQUE :** Vous devez disposer de l'autorisation **Exécuter les commandes d'action du serveur** pour effectuer les actions de gestion de l'alimentation. Consultez [Ajout et configuration d'utilisateurs iDRAC6](#) pour obtenir de l'aide sur la configuration des droits d'utilisateur.

1. Cliquez sur **Système**, puis sur **Gestion de l'alimentation** → **onglet Contrôle de l'alimentation**.
2. Sélectionnez une **opération de contrôle de l'alimentation**, par exemple **Réinitialiser le système (redémarrage à chaud)**. [Tableau 19-12](#) fournit des informations sur les actions de contrôle de l'alimentation.
3. Cliquez sur **Appliquer** pour effectuer l'action sélectionnée.

Tableau 19-12. Actions de contrôle de l'alimentation

Allumer le système	Met le système sous tension (comme si vous appuyiez sur le bouton d'alimentation lorsque le système est hors tension).
Arrêter le système	Met le système hors tension (comme si vous appuyiez sur le bouton d'alimentation lorsque le système est sous tension).
NMI (interruption non masquable)	Envoie une interruption de niveau élevé au système d'exploitation, qui par conséquent arrête les opérations pour permettre des activités de diagnostic ou de dépannage critiques.
Arrêt normal	Tente d'arrêter le système d'exploitation correctement, puis met hors tension le système. Ceci nécessite que le système d'exploitation prenne en charge l'interface ACPI afin de contrôler la gestion de l'alimentation système. REMARQUE : Un arrêt normal du système d'exploitation du serveur n'est parfois pas possible lorsque le logiciel du serveur cesse de répondre ou si aucun administrateur n'a ouvert de session sur la console locale d'un système Windows. Dans ces cas, vous devez demander le redémarrage forcé de Windows au lieu d'un arrêt normal. De plus, selon la version du système d'exploitation Windows, une stratégie peut être configurée autour du processus d'arrêt et risque de modifier le comportement de l'arrêt lorsqu'il est déclenché à partir d'iDRAC6. Consultez la documentation de Microsoft pour connaître la règle de l'ordinateur local « Arrêt : autoriser l'arrêt du système sans avoir à ouvrir une session ».
Réinitialiser le système (démarrage à chaud)	Redémarre le système sans le mettre hors tension (redémarrage à chaud).
Exécuter un cycle d'alimentation du	Met le système hors tension, puis le redémarre (redémarrage à froid).

Pour plus d'informations, consultez la section [Contrôle et gestion de l'alimentation](#).

Dépannage et questions les plus fréquentes

Tableau 19-13 contient les questions les plus fréquentes sur les problèmes de dépannage.

Tableau 19-13. Questions les plus fréquentes/Dépannage

Question	Réponse
La LED présente sur le serveur clignote en orange.	<p>Vérifiez les messages du journal SEL, puis effacez-les pour arrêter la LED qui clignote.</p> <p>À partir de l'interface Web iDRAC6 :</p> <ol style="list-style-type: none"> 1. Consultez « Vérification du journal des événements système (SEL) » <p>À partir de la commande SM-CLP :</p> <ol style="list-style-type: none"> 1. Consultez Gestion du journal SEL <p>À partir de l'utilitaire de configuration iDRAC6 :</p> <ol style="list-style-type: none"> 1. Consultez Menu Journal des événements système
Une LED bleue clignote sur le serveur.	<p>Un utilisateur a activé la référence de l'indicateur d'emplacement pour le serveur. Il s'agit d'un signal leur permettant d'identifier le serveur dans le châssis. Consultez Identification du serveur géré dans le châssis pour obtenir des informations sur cette fonctionnalité.</p>
Comment puis-je trouver l'adresse IP d'iDRAC6 ?	<p>Depuis l'interface Web CMC :</p> <ol style="list-style-type: none"> 1. Cliquez sur Châssis → Serveurs, puis cliquez sur l'onglet Configuration. 2. Cliquez sur Déployer. 3. Lisez l'adresse IP de votre serveur dans le tableau affiché. <p>Depuis la console virtuelle :</p> <ol style="list-style-type: none"> 1. Redémarrez le serveur et entrez dans l'utilitaire de configuration iDRAC6 en appuyant sur <Ctrl><E> 1. Surveillez l'affichage de l'adresse IP lors du POST du BIOS. 1. Sélectionnez la console « Dell CMC » dans OSCAR afin de vous connecter à CMC via une connexion série locale. Les commandes RACADM CMC peuvent être émises à partir de cette connexion. Consultez le <i>Guide de référence de l'administrateur Dell Chassis Management Controller</i> pour accéder à la liste complète des sous-commandes RACADM CMC. 1. Utilisez la commande RACADM locale getsysinfo pour afficher l'adresse IP d'iDRAC6.
	<p>Par exemple :</p> <pre>\$ racadm getniccfg -m server-1</pre> <p>DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1</p> <p>À partir d'une commande RACADM locale :</p> <p>Entrez la commande suivante à l'invite de commande :</p> <pre>racadm getsysinfo</pre> <p>À partir de l'écran LCD :</p> <ol style="list-style-type: none"> 1. Sur le menu principal, mettez en surbrillance Serveur et appuyez sur le bouton de vérification. 2. Sélectionnez le serveur dont vous recherchez l'adresse IP et appuyez sur le bouton de vérification.
Comment puis-je trouver l'adresse IP de CMC ?	<p>À partir de l'interface Web iDRAC6 :</p> <ol style="list-style-type: none"> 1. Cliquez sur Système → Accès à distance → CMC. <p>L'adresse IP CMC s'affiche dans l'écran Résumé CMC.</p> <p>Depuis la console virtuelle :</p> <ol style="list-style-type: none"> 1. Sélectionnez la console « Dell CMC » dans OSCAR afin de vous connecter à CMC via une connexion série locale. Les commandes RACADM CMC peuvent être émises à partir de cette connexion. Reportez-vous au <i>Guide de référence de l'administrateur Dell Chassis Management Controller</i> pour accéder à la liste complète des sous-commandes RACADM CMC. <pre>\$ racadm getniccfg -m chassis</pre>

	<p>NIC Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate</p> <p>REMARQUE : L'action ci-dessus peut uniquement être effectuée avec la RACADM distante.</p>
La connexion réseau iDRAC6 ne fonctionne pas.	<ul style="list-style-type: none"> 1. Assurez-vous que le câble LAN est connecté à CMC. 1. Assurez-vous que les paramètres NIC, les paramètres IPv4 ou IPv6 et que Statique ou DHCP est activé pour votre réseau.
J'ai inséré le serveur dans le châssis et j'ai appuyé sur le bouton d'alimentation, mais rien ne s'est produit.	<ul style="list-style-type: none"> 1. iDRAC6 nécessite jusqu'à 2 minutes pour s'initialiser avant la mise sous tension du serveur. 1. Vérifiez le bilan de puissance CMC. Le bilan de puissance du châssis a peut-être été dépassé.
J'ai oublié le nom d'utilisateur et le mot de passe d'administration iDRAC6.	<p>Vous devez rétablir les paramètres par défaut d'iDRAC6.</p> <ol style="list-style-type: none"> 1. Redémarrez le serveur et appuyez sur <Ctrl><E> lorsque le système vous y invite afin d'entrer dans l'utilitaire de configuration iDRAC6. 2. Dans le menu Utilitaire de configuration iDRAC6, mettez en surbrillance Restaurer les paramètres par défaut et appuyez sur <Entrée>. <p>REMARQUE : Vous pouvez également réinitialiser iDRAC6 à partir de la RACADM locale en émettant la commande <code>racadm racresetcfg</code>.</p> <p>Pour plus d'informations, consultez Rétablir les paramètres par défaut.</p>
Comment puis-je changer le nom du logement de mon serveur ?	<ol style="list-style-type: none"> 1. Ouvrez une session sur l'interface Web CMC. 2. Ouvrez l'arborescence du châssis et cliquez sur Serveurs. 3. Cliquez sur l'onglet Configuration. 4. Entrez le nouveau nom du logement dans la ligne correspondant à votre serveur. 5. Cliquez sur Appliquer.
Lors du démarrage d'une session de console virtuelle à partir de l'interface Web iDRAC6, un message contextuel de sécurité ActiveX apparaît.	<p>iDRAC6 n'est peut-être pas un site sécurisé. Pour empêcher l'affichage du message contextuel de sécurité à chaque démarrage d'une session de console virtuelle, ajoutez iDRAC6 à la liste des sites sécurisés dans le navigateur client :</p> <ol style="list-style-type: none"> 1. Cliquez sur Outils → Options Internet → Sécurité → Sites de confiance. 2. Cliquez sur Sites et entrez l'adresse IP ou le nom DNS d'iDRAC6. 3. Cliquez sur Ajouter. 4. Cliquez sur Personnaliser le niveau. 5. Dans la fenêtre Paramètres de sécurité, sélectionnez Demander sous Télécharger les contrôles ActiveX non signés.
Lorsque je démarre une session de console virtuelle, l'écran du visualiseur est vierge.	<p>Si vous disposez du privilège Média virtuel mais pas du privilège Console virtuelle, vous êtes en mesure de démarrer le visualiseur afin de pouvoir accéder à la fonctionnalité de média virtuel mais la console du serveur géré ne s'affichera pas.</p>
iDRAC6 se bloque au cours du démarrage.	<p>Retirez et réinsérez le serveur.</p> <p>Contrôlez l'interface Web CMC afin de déterminer si iDRAC6 apparaît en tant que composant pouvant être mis à niveau. Si tel est le cas, suivez les instructions dans Mise à jour du micrologiciel iDRAC6 avec CMC.</p> <p>Si ceci ne corrige pas le problème, contactez le support technique.</p>
Lors de la tentative de démarrage du serveur géré, le voyant d'alimentation est vert, mais aucun POST ou aucune vidéo ne s'affiche.	<p>Cela peut se produire si l'une des conditions suivantes est réunie :</p> <ul style="list-style-type: none"> 1. La mémoire n'est pas installée ou est inaccessible. 1. L'UC n'est pas installée ou est inaccessible. 1. La carte adaptatrice de connexion vidéo est manquante ou incorrectement connectée. <p>En outre, recherchez les messages d'erreur dans le journal iDRAC6 à partir de l'interface Web iDRAC6 ou de l'écran LCD.</p>

[Retour à la page du sommaire](#)