Integrated Dell Remote Access Controller 7 (iDRAC7)
Guide d'utilisation de la version 1.50.50

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessure corporelle ou de mort.

2013 - 12

Rev. A00

Table des matières

1

Présentation

iDRAC (Integrated Dell Remote Access Controller 7) a pour vocation d'améliorer la productivité des administrateurs et la disponibilité générale des serveurs Dell. iDRAC7 signale aux administrateurs les incidents des serveurs, les aide à gérer à distance les serveurs et réduit le besoin d'accéder physiquement au serveur.

iDRAC7, avec la technologie Lifecycle Controller, fait partie d'une grande solution de centre de données qui permet de maintenir disponible en permanence les applications et les charges de travail stratégiques. Avec cette technologie, les administrateurs peuvent déployer, surveiller, gérer, configurer, mettre à jour, dépanner et réparer les serveurs Dell depuis n'importe quel emplacement et sans utiliser des agents. Ces opérations sont possibles, qu'un système d'exploitation ou un hyperviseur soit présent ou non ou quel que soit l'état du système d'exploitation ou de l'hyperiseur.

Plusieurs produits fonctionnent avec iDRAC7 et Lifecycle Controller pour simplifier et rationaliser les opérations informatiques :

- Dell Management Plug-In pour VMware vCenter
- Dell Repository Manager
- Dell Management Packs pour Microsoft System Center Operations Manager (SCOM) et Microsoft System Center Configuration Manager (SCCM)
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

Il existe les variantes suivantes d'iDRAC7 :

- Gestion de base avec IPMI (disponible par défaut sur les serveurs de série 200-500)
- iDRAC7 Express (disponible par défaut sur tous les serveurs en rack et de type tour de série 600 et ultérieure et sur tous les serveurs lame)
- iDRAC7 Enterprise (disponible sur tous les modèles de serveur)

Pour plus d'informations, voir le *iDRAC7 Overview and Feature Guide* (Guide de présentation et des fonctions iDRAC7) disponible à l'adresse **dell.com/support/manuals**.

Avantages de l'utilisation d'iDRAC7 avec Lifecycle Controller

Avantages :

- Amélioration de la disponibilité : notification anticipéée des échecs potentiels ou réels pour empêcher une défaillance d'un serveur ou réduire le temps de récupération après un incident.
- Amélioration de la productivité et réduction du coût total de possession : comme les administrateurs peuvent accéder à un plus grand nombre de serveurs distants, le personnel informatique est plus productif et les coûts opérationnels, tels que les déplacements, sont réduits.
- Environnement sécurisé : en fournissant un accès sécurisé aux serveurs distants les administrateurs peuvent exécuter des fonctions de gestion importantes sans affecter la sécurité des serveurs et du réseau.
- Gestion intégrée étendue via le Lifecycle Controller : le Lifecycle Controller fournit des fonctions de déploiement et de maintenance simplifiée via l'interface graphique Lifecycle Controller pour le déploiement local, et des interfaces (Gestion WS) de services à distance intégrées à Dell OpenManage Essentials et aux consoles partenaires.

Pour plus d'informations sur l'interface graphique utilisateur Lifecycle Controller, voir le *Lifecycle Controller User's Guide* (Guide d'utilisation du Lifecycle Controller). Pour les services distants, voir le *Lifecycle Controller Remote Services User's Guide* (Guide d'utilisation des services à distance Lifecycle Controller) disponible à l'adresse **dell.com/support/manuals**.

Principales fonctions

Principales fonctions disponibles dans iDRAC7 :

REMARQUE : Certaines fonctions sont disponibles uniquement avec la licence iDRAC7 Enterprise. Pour en savoir plus sur les fonctions disponibles pour une licence, voir Gestion des licences.

Inventaire et surveillance

- Affichage de l'intégrité des serveurs.
- Effectuez l'inventaire et surveillez les adaptateurs de réseau et les sous-systèmes de stockage (PERC et stockage directement relié) sans agent de système d'exploitation.
- Affichez et exportez l'inventaire du système.
- Affichez les informations sur le capteur, telles que la température, la tension et l'intrusion.
- Surveillez l'état de l'UC, la limitation automatique du processeur et les échecs prévisibles.
- Affichez les informations relatives à la mémoire.
- Surveillance et contrôle de l'utilisation de l'alimentation
- Prise en charge des opérations get SNMPv3.
- Pour les serveurs lames, lancement de l'interface Web CMC (Chassis Management Controller), affichage des informations CMS et des adresses WWN/MAC.

  REMARQUE : CMC permet d'accéder à iDRAC7 via le panneau LCD du châssis M1000E et des connexions de console locales. Pour plus d'informations, voir le document *Chassis Management Controller User's Guide* (Guide d'utilisation de Chassis Management Controller) disponible à l'adresse **dell.com/support/manuals**.

Déploiement

- Gestion des partitions de carte SD vFlash SD
- Configuration des paramètres de l'écran du panneau avant
- Lancement du Lifecycle Controller qui permet de configurer et de mettre à jour le BIOS et les cartes réseau et de stockage compatibles.
- Gestion des paramètres réseau iDRAC7
- Configuration et utilisation d'une console virtuelle de média virtuel
- Déploiement de systèmes d'exploitation en utilisant le partage de fichier à distance, média virtuel et VMCLI.
- Activation de l'auto-détection.
- Effectuez la configuration du serveur à l'aide de la fonction d'exportation ou d'importation du profil XML via RACADM et WS-MAN. Pour en savoir plus, voir le *Lifecycle Controller Remote Services Quick Start Guide* (Guide de démarrage rapide des services à distance du Lifecycle Controller).

Mettre à jour

- Gestion des licences iDRAC7.
- Mettre à jour le BIOS et le micrologiciel de périphérique des périphériques pris en charge par le Lifecycle Controller
- Mise à jour et restauration du micrologiciel d'iDRAC7
- Gérer les mises à jour étagées.
- Profil du serveur de sauvegarde et de restauration

Maintenance et dépannage

- Exécution d'opérations d'alimentation et surveillance de la consommation d'énergie.
- Aucune dépendance de l'administrateur de serveur pour la génération d'alertes
- Journalisation des données d'événements : journaux Lifecycle et journaux RAC
- Définition des alertes par e-mail, alertes IPMI, journaux de système distant, journaux d'événements WS et interruptions SNMP (v1 et v2c) pour des événements et notification d'alerte par e-mail optimisée.
- Capture de la dernière image de blocage du système
- Affichage des vidéos de capture du démarrage et du blocage.

Sécurisation des connexions

La sécurisation de l'accès aux ressources réseau stratégiques est une priorité. iDRAC7 met en œuvre diverses fonctions de sécurité, notamment :

- Certificat de signature personnalisé pour le certificat SSL (couche de sockets sécurisé).
- Mises à jour signées du micrologiciel
- Authentification utilisateur via Microsoft Active Directory, service de répertoire LDAP (Lightweight Directory Access Protocol - Protocole d'accès aux annuaires allégé) générique, ou ID et mots de passe utilisateur administrés localement.
- Authentification bifactorielle en utilisant la fonction de connexion par carte à puce. Cette authentification repose sur la carte à puce physique et son code PIN.
- Connexion directe et authentification par clé publique.
- Autorisation basée sur le rôle pour définir des privilèges pour chaque utilisateur
- L'authentification SNMPv3 pour les comptes utilisateur stockés localement dans l'iDRAC. Il est recommandé de l'utiliser, cependant celle-ci est désactivée par défaut.
- Configuration de la référence utilisateur et du mot de passe
- Modification du mot de passe d'ouverture de session par défaut.
- Interfaces SMCLP 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
- Configuration du délai d'expiration de la session (en secondes)
- Ports IP configurables (pour HTTP, HTTPS, SSH, Telnet, la console virtuelle et Média Virtuel).

  REMARQUE : Telnet ne prend pas en charge le cryptage SSL et il est désactivé par défaut
- SHH (Secure Shell) qui utilise une couche de transport cryptée pour une sécurité accrue.
- Nombre maximal d'échecs de connexion par adresse IP, avec blocage de connexion à partir de cette adresse IP lorsque la limite est dépassée
- Plage d'adresses IP limitée pour les clients se connectant à iDRAC7
- Adaptateur Ethernet Gigabit dédié pour les serveurs en rack ou de type tour avec licence d'entreprise.

Nouveautés de cette version

Voici les nouvelles fonctionnalités de cette version :

- Configuration automatique des composants dans un serveur ou plusieurs serveurs à l'aide du provisionnement DHCP et des fichiers de configuration XML auxquels iDRAC accède à partir d'un partage réseau.
- Planification automatique des mises à jour du micrologiciel auxquelles iDRAC accède à partir d'un partage réseau ou site FTP.
- Mise à jour manuelle du micrologiciel à l'aide d'un fichier image de micrologiciel stocké sur un système local ou sur un partage réseau, en le connectant à un site FTP ou un espace de stockage réseau qui contient un catalogue des mises à jour disponibles.
- Annulation des mises à jour du micrologiciel pour tous les périphériques pris en charge par Lifecycle Controller.

- Configuration et planification des sauvegardes de configuration du serveur.
- Activation ou désactivation des redirections HTTP.
- Configuration du serveur VNC pour voir le bureau à distance à l'aide de périphériques mobiles.
- Configuration du LOM ou de la carte réseau USB comme canal de passage du système d'exploitation à iDRAC.
- Activation ou désactivation de l'optimisation des E/S.
- Activation de la journalisation des événements dans les journaux du système d'exploitation (SE).
- Exportation des entrées du journal Lifecycle dans un partage réseau ou sur le système local.
- Amélioration des options de menu **Média virtuel** :
  - Connexion ou déconnexion de session de média virtuel à partir du menu **Média virtuel**.
  - Spécification de l'emplacement du fichier image créé à partir du dossier.
  - Création d'une image à partir du dossier sans activer la session Média virtuel.
  - Nouvelle interface lorsque le média virtuel est lancé en mode autonome.
- Statistiques de performances de média virtuel détaillées combinées avec les statistiques de console virtuelle dans la boîte de dialogue **Statistiques**.
- RFS supprimé de la liste des périphériques d'armorçage initial et suivant.
- Effacement des journaux d'événements système.
- Affichage des journaux d'événements système dans l'utilitaire des paramètres iDRAC.
- Consignation des ouvertures et fermetures de session et des événements d'échec de connexion dans les journaux Lifecycle Controller.
- Stockage permanent du certificat dans le magasin de certificats de l'utilisateur.
- Désactivation des messages d'avertissement pendant le lancement de la console virtuelle ou du média virtuel à l'aide du plug-in Java ou ActiveX.
- Amélioration des options de **partage de fichiers à distance**.
- Utilisation du module de service iDRAC pour effectuer les fonctions d'analyse similaires à celles de Server Administrator, mais dans un environnement hors bande.
- Configuration de ports SNMP et SMTP.
- Planification automatique des diagnostics à distance.
- Mise sous ou hors tension du voyant du panneau avant à partir de la page **Résumé du système**.
- Utilisation de certificats génériques.
- Utilisation de certificats signés par une autorité de certification intermédiaire (CA).
- Création d'un rapport de support technique similaire à ceux de l'outil de support électronique du système Dell.
- Affichage des informations suivantes pour les périphériques de stockage :
  - Réglage de la taille des secteurs que les disques physiques et les disques virtuels utilisent pour stocker les données.
  - Expiration du niveau ou de la durée de vie restante du SSD (solid-state drive) connecté à un contrôleur PERC.
  - Lecteurs conformes Protection Information T10 (PI) pris en charge par les contrôleurs.
  - Fonction PI T10 pour les disques physiques.
  - Fonction PI T10 activée ou désactivée pour le disque virtuel.
  - Prise en charge du mode d'amorçage du contrôleur pour les contrôleurs.
  - Importation automatique des configurations étrangères améliorée activée ou désactivée pour le contrôleur.
  - Matrices avec prise en charge de différentes longueurs de répartition pour les disques virtuels RAID 10.

Comment utiliser ce Guide d'utilisation

Le contenu de ce guide d'utilisation vous permet d'exécuter les tâches en utilisant :

- L'interface Web iDRAC7 : seules les informations liées aux tâches sont fournies ici. Pour des informations concernant les champs et les options, voir l'*Aide en ligne d'iDRAC7*, accessible depuis l'interface Web.
- RACADM : La commande RACADM ou l'objet que vous devez utiliser se trouvent ici. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM* disponible sur le site **dell.com/support/manuals**.
- L'utilitaire de configuration d'iDRAC : seules les informations liées aux tâches sont fournies ici. Pour des informations concernant les champs et les options, voir l'*Aide en ligne de l'utilitaire Paramètres d'iDRAC7*, accessible en cliquant sur **Aide** dans l'interface GUI des paramètres d'iDRAC (appuyez sur <F2> lors du démarrage, puis cliquez sur **Paramètres d'iDRAC** à la page **Menu principal de configuration du système**).

Navigateurs Web pris en charge

iDRAC7 est pris en charge sur les navigateurs pris en charge :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Pour une liste des versions, voir le fichier *Lisez-moi* disponibles à l'adresse **dell.com/support/manuals**.

Gestion des licences

Les fonctions iDRAC7 sont disponibles en fonction de la licence (Gestion de base, iDRAC7 Express, ou iDRAC7 Enterprise) achetée. Seules les fonctions sous licence sont disponibles dans les interfaces qui permettent de configurer ou d'utiliser iDRAC7, par exemple, l'interface Web iDRAC7, l'interface RACADM ou l'interface WS-MAN, OpenManage Server Administrator, etc. Certaines fonctions, telles que NIC dédié ou vFlash, nécessitent une carte de ports iDRAC qui est disponible en option sur les serveurs 200-500.

La fonctionnalité iDRAC7 de gestion des licences et de mise à jour du microproligiciel est toujours disponible via l'interface Web d'iDRAC7 et l'interface RACADM.

Types de licences

Les types de licences proprosés sont les suivants :

- Évaluation de 30 jours et extension : la licence expire au bout de 30 jours. La période d'évaluation peut être prolongée de 30 jours. Les licences d'évaluation reposent sur la durée et le décompte du temps démarre lorsque le système est mis sous tension.
- Perpétuelle : la licence est liée au numéro de service et elle est prermanente.

Obtention de licences

Pour obtenir des licences, procédez de l'une des manières suivantes :

- E-mail : la licence est jointe à un e-mail envoyé après sa demande auprès du centre d'assistance technique.
- Portail de libre service : un lien vers le portail de libre service est disponible depuis l'iDRAC7. Cliquez sur ce lien pour ouvrir le portail de libre service sur Internet. Vous pouvez actuellement utiliser le portail de libre service pour obtenir les licences achetées avec le serveur. Vous devez contacter le représentant commercial ou le support technique pour acheter une nouvelle licence ou mettre à niveau une licence. Pour en savoir plus, voir l'aide en ligne pour la page du portail de libre service.
- Point de vente : la licence est acquise lors de la commande d'un système.

Opérations de licence

Avant d'exécuter les tâches de gestion des licences, veillez à obtenir les licences. Pour plus d'informations, voir le document *Overview and Feature Guide* (Guide de présentation et des fonctions) disponible à l'adresse **dell.com/support/manuals**.

REMARQUE : Si vous avez acheté un système avec toutes les licences préinstallées, la gestion des licences n'est pas nécessaire.

Vous pouvez exécuter les opérations de licence suivantes en utilisant iDRAC7, RACADM, WS-MAN et Lifecycle Controller-Services distants pour la gestion de licence individuelle, et Dell License Manager pour la gestion un-à plusieurs des licences :

- Afficher : affichage des informations de la licence en cours.
- Importer : après l'acquisition d'une licence, stockez la licence dans un emplacement de stockage local et importez-la vers iDRAC7 en utilisant l'une des interfaces prises en charge. La licence est importée si les vérifications de validation auxquelles elle est soumise aboutissent.

  REMARQUE : Pour un nombre limité de fonctions, il est nécessaire de redémarrer le système pour activer les fonctions.
- Exporter : exporte la licence installée vers un périphérique de stocklage externe pour disposer d'une sauvegarde ou la réinstaller après le remplacement d'un composant ou de la carte-mère. Le nom de fichier et le format d'une licence exportée sont **<EntitlementID>.xml**.
- Supprimer : supprime la licence affectée à un composant si le composant manque. Une fois la licence supprimée, elle n'est plus stockée dans iDRAC7 et les fonctions de base du produit sont activées.
- Remplacer : remplacement de la licence pour prolonger la période d'évaluation d'une licence, changer le type de licence (remplacement d'une licence d'évaluation par une licence achetée) ou étendre une licence expiré.
  - Une licence d'évaluation peut être remplacée par une licence d'évaluation mise à niveau ou une licence achetée.
  - Une licence achetée peut être remplacée par une licence mise à niveau ou une licence mise à jour.
- En savoir plus : en savoir plus sur une licence installée ou les licences disponibles pour un composant installé sur le serveur.

  REMARQUE : Pour que l'option En savoir plus affiche la page correcte, veillez à ajouter ***.dell.com** à la liste des sites de confiance dans les paramètres de sécurité. Pour plus d'informations, voir la documentation d'aide d'Internet Explorer.

Pour le déploiement de licence un à plusieurs, vous pouvez utiliser Dell License Manager. Pour plus d'informations, voir le *Dell License Manager User's Guide* (Guide d'utilisation de Dell License Manager) disponible à l'adresse **dell.com/support/manuals**.

Importation de la licence suite au remplacement de la carte mère

Vous pouvez utiliser l'outil d'installation locale de la licence iDRAC7 Enterprise si vous avez récemment remplacé la carte mère et avez besoin de réinstaller la licence iDRAC7 Enterprise localement (sans aucune connectivité réseau) et d'activer la carte réseau dédiée. Cet utilitaire installe une licence iDRAC7 Enterprise d'évaluation d'une durée de 30 jours et vous permet de réinitialiser l'iDRAC pour passer d'une carte réseau partagée à une carte réseau dédiée.

Pour en savoir plus sur cet utilitaire et pour télécharger cet outil, cliquez ici.

État ou condition de composant de licence et opérations disponibles

Le tableau suivant répertorie les opérations de licence disponibles en fonction de l'état ou de la condition d'une licence.

Tableau 1. Opérations de licence en fonction de l'état et de la condition

État/Condition ou état du composant	Importer	Exporter	Supprimer	Remplacer	En savoir plus
Connexion non-administrateur	Non	Non	Non	Non	Oui
Licence active	Oui	Oui	Oui	Oui	Oui
Licence expirée	Non	Oui	Oui	Oui	Oui
License installée, mais composant manquant	Non	Oui	Oui	Non	Oui

Gestion des licences à l'aide de l'interface Web d'iDRAC7

Pour gérer les licences à l'aide de l'interface Web d'iDRAC7, accédez à **Présentation** → **Serveur** → **Licences** .

La page **Gestion des licences** affiche les licences associées à des périphériques ou les licences installées des périphériques absent du système. Pour plus d'informations sur l'importation, l'exportation, la suppression ou le remplacement d'une licence, voir l'*aide en ligne d'iDRAC7*.

Gestion des licences à l'aide de l'interface RACADM

Pour gérer les licences à l'aide de l'interface RACADM, utilisez la sous-commande **licence**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible sur le site **support.dell.com/manuals**.

Fonctions utilisables sous licence dans iDRAC7

Le tableau suivant répertorie les fonctions iDRAC7 qui sont activées en fonction de la licence achetée.

Tableau 2. Fonctions iDRAC7 utilisables sous licence

Fonction	Basic Management avec IPMI	iDRAC7 Express (serveurs en rack et de type tour)	iDRAC7 Express (serveurs lame)	iDRAC7 Enterprise
Prise en charge d'interface et des normes				
IPMI 2.0	Oui	Oui	Oui	Oui
Interface Web [1]	Non	Oui	Oui	Oui
SNMP	Non	Oui	Oui	Oui
WS-MAN	Oui	Oui	Oui	Oui
SMASH-CLP (SSH)	Non	Oui	Oui	Oui
Interface RACADM (SSH, locale et distante) [1]	Non	Oui	Oui	Oui
Telnet	Non	Oui	Oui	Oui
Connectivité				
Mode partagé ou réseau de basculement (serveurs en rack et de type tour uniquement)	Oui	Oui	Non	Oui

Fonction	Basic Management avec IPMI	iDRAC7 Express (serveurs en rack et de type tour)	iDRAC7 Express (serveurs lame)	iDRAC7 Enterprise
NIC dédié	Non	Non	Oui [2]	Oui [2,6]
DNS	Oui	Oui	Oui	Oui
Marquage VLAN	Oui	Oui	Oui	Oui
IPv4	Oui	Oui	Oui	Oui
IPv6	Non	Oui	Oui	Oui
DNS dynamique	Non	Oui	Oui	Oui
Sécurité et authentification				
Autorité basée sur les rôles	Oui	Oui	Oui	Oui
Utilisateurs locaux	Oui	Oui	Oui	Oui
Services d'annuaire (Active Directory et LDAP générique)	Non	Non	Non	Oui
Cryptage SSL	Oui	Oui	Oui	Oui
Authentification bifactorielle [3]	Non	Non	Non	Oui
Connexion directe SSO (Single Sign-On)	Non	Non	Non	Oui
Authentification PK (pour SSH)	Non	Non	Non	Oui
Verrouillage de sécurité	Non	Oui	Oui	Oui
Gestion et conversion à distance				
Diagnostic intégré	Oui	Oui	Oui	Oui
Communications série sur LAN (avec proxy)	Oui	Oui	Oui	Oui
Communications série sur LAN (sans proxy)	Non	Oui	Oui	Oui
Capture d'écran de blocage	Non	Oui	Oui	Oui
Capture de vidéo de blocage	Non	Non	Non	Oui
Capture au démarrage	Non	Non	Non	Oui
Média virtuel [4]	Non	Non	Oui	Oui
Console virtuelle [4]	Non	Non	Oui [5]	Oui
Collaboration console [4]	Non	Non	Non	Oui
Dossier virtuel	Non	Non	Non	Oui
Discussion console virtuelle	Non	Non	Non	Oui
Partage de fichier à distance	Non	Non	Non	Oui
vFlash [6]	Non	Non	Non	Oui
Partitions vFlash [6]	Non	Non	Non	Oui
Détection automatique	Non	Oui	Oui	Oui
Sauvegarde d'un profil de serveur	Non	Non	Non	Oui

Fonction	Basic Management avec IPMI	iDRAC7 Express (serveurs en rack et de type tour)	iDRAC7 Express (serveurs lame)	iDRAC7 Enterprise
Remplacement de pièces [8]	Non	Oui	Oui	Oui
Protocole de temps de réseau (NTP)	Non	Oui	Oui	Oui
Mises à jour planifiées	Non	Non	Non	Oui
Serveur VNC	Non	Non	Non	Oui
Surveillance et alimentation				
Surveillance et alertes des capteurs	Oui	Oui	Oui	Oui
Surveillance des périphériques	Non	Oui	Oui	Oui
Suveillance du stockage	Non	Oui	Oui	Oui
Capteurs d'UC et de mémoire individuels	Oui	Oui	Oui	Oui
Alertes par e-mail	Non	Oui	Oui	Oui
Compteurs d'alimentation historiques	Oui	Oui	Oui	Oui
Plafonnement de l'alimentation	Non	Non	Non	Oui
Contrôle de l'alimentation en temps réel	Oui	Oui	Oui	Oui
Graphique d'alimentation en temps réel	Non	Oui	Oui	Oui
Module de service iDRAC	Non	Oui	Oui	Oui
Rapport du Support technique	Non	Oui	Oui	Oui
Journalisation				
Journal des événements système	Oui	Oui	Oui	Oui
Journal RAC [7]	Non	Oui	Oui	Oui
Journal de trace [7]	Non	Oui	Oui	Oui
Syslog distant	Non	Non	Non	Oui

[1] La mise à jour du micrologiciel et la gestion des licences iDRAC7 sont toujours disponibles via l'interface Web et l'interface d'iDRAC7.

[2] Tous les serveurs lames utilisent un NIC dédié pour iDRAC7 en permanence, mais la vitesse est limitée à 100 Mbps. La carte GIGABYTE Ethernet ne fonctionne pas sur les serveurs lames du fait des limitations du châssis, mais elle fonctionne sur les serveurs en rack et de type tour avec une licence d'entreprise. LOM partagé n'est pas activé sur les serveurs lames.

[3] L'authentification bifactorielle est disponible via Active-X et elle prend donc uniquement en charge Internet Explorer.

[4] La console virtuelle et Média virtuel sont disponibles via les plug-ins Java et Active-X.

[5] Console virtuelle utilisateur unique avec lancement à distance.

[6] Sur certains systèmes les cartes iDRAC7 en option sont nécessaires.

[7] Les journaux RAC et de trace sont disponibles dans la version de base via WS-MAN.

[8] La fonction Remplacement de pièce du Lifecycle Controller simplifie le processus de remplacement d'une pièce défaillante en restaurant le niveau du micrologiciel et la configuration de la pièce de remplacement. Pour en savoir plus, voir le *Dell Lifecycle Controller User's Guide* (Guide d'utilisation du Dell LifeCycle Controller) disponible à l'adresse **dell.com/support/manuals**.

Interfaces et protocoles d'accès à iDRAC7

Le tableau suivant répertorie les interfaces d'accès à iDRAC7.

REMARQUE : L'utilisation simultanée de plusieurs interfaces de configuration peut générer des résultats inattendus.

Tableau 3. Interfaces et protocoles d'accès à iDRAC7

Interface ou protocole	Description
Utilitaire iDRAC Settings (Configuration iDRAC)	Utilisez l'utilitaire de configuration d'iDRAC pour exécuter des opérations de pré-système d'exploitation. Il inclut un sous-groupe de fonctions disponibles dans l'interface Web d'iDRAC7 et d'autres fonctions. Pour accéder à l'utilitaire de configuration d'iDRAC, appuyez sur <F2> pendant le démarrage et cliquez sur **Paramètres iDRAC** dans la page du **menu principal de la configuration du système**.
Interface Web iDRAC7	Utilisez l'interface Web d'iDRAC7 pour gérer iDRAC7 et surveiller le système géré. Le navigateur se connecte au serveur Web via le port HTTPS. Les flux de données sont cryptés en utilisant SSL 128 bits pour protéger les données personnelles et l'intégrité. Les connexions au port HTTP sont redirigées vers HTTPS. Les administrateurs peuvent téléverser leur propre certificat SSL via un processus de génération RSC SSL pour sécuriser le serveur Web. Les ports par défaut HTTP et HTTPS peuvent être changés. L'accès utilisateur repose sur des privilèges d'utilisateur.
RACADM	Utilisez cet utilitaire de ligne de commande pour exécuter des opérations iDRAC7 et de gestion de serveur. Vous pouvez utiliser RACADM localement et à distance. • L'interface de ligne de commande RACADM s'exécute sur les systèmes gérés disposant de Server Administrator. L'interface RACADM locale communique avec iDRAC7 via son interface hôte IPMI intrabande. Comme elle est installée sur le système géré local, les utilisateurs doivent se connecter au système d'exploitation pour pouvoir exécuter cet utilitaire. Un utilisateur doit avoir tous les privilèges d'administrateur ou doit être un utilisateur root pour pouvoir utiliser l'utilitaire. • L'interface distante RACADM est un utilitaire client exécuté sur une station de gestion. Elle utilise l'interface réseau hors bande pour exécuter des commandes RACADM sur le système géré et le canal HTTPs. Les options **–r** exécutent la commande RACADM sur un réseau. • Le micrologiciel RACADM est accessible en se connectant à iDRAC7 en utilisant SSH ou telnet. Vous pouvez exécuter les commandes du micrologiciel RACADM sans définir d'adresse, de nom d'utilisateur ou de mot de passe iDRAC7. • Il est inutile de définir l'adresse IP, le nom d'utilisateur ou le mot de passe iDRAC7 IP pour exécuter les commandes du micrologiciel RACADM. Une fois dans l'invite RACADM, vous pouvez exécuter les commandes directement sans le préfixe racadm.
Panneau LCD du serveur/Panneau LCD du châssis	Utilisez l'écran LCD du panneau avant du serveur pour : • afficher les alertes, l'adresse iDRAC7 ou l'adresse MAC, des chaînes programmables par l'utilisateur ; • définir DHCP ; • configurer les paramètres IP statiques iDRAC7. Dans le cas des serveurs lames, l'écran LCD se trouve sur le panneau avant du châssis et il est partagé entre tous les serveurs lames.

Interface ou protocole	Description
	Pour réinitialiser iDRAC sans redémarrer le serveur, appuyez sur le bouton d'identification système et maintenez-le enfoncé pendant 16 secondes.
Interface Web CMC	Outre la surveillance et la gestion du châssis, utilisez l'interface Web CMC pour : • afficher l'état d'un système géré ; • mettre à jour le micrologiciel iDRAC7 ; • configurer les paramètres réseau iDRAC7 ; • vous connecter à l'interface Web iDRAC7 ; • démarrer, arrêter ou réinitialiser le système géré ; • mettre à jour le BIOS, PERC et les adaptateurs réseau pris en charge.
Lifecycle Controller	Utilisez le Lifecycle Controller pour effectuer des configurations iDRAC7. Pour accéder au Lifecycle Controller, appuyez sur <F10> au cours du démarrage et accédez à **Configuration du système → Configuration matérielle avancée → Paramètres iDRAC** . Voir le *Lifecycle Controller User's Guide* (Guide d'utilisation du Lifecycle Controller), est disponible à l'adresse **dell.com/support/manuals**.
Telnet	Utilisez Telnet pour accéder à iDRAC7 où vous pouvez exécuter des commandes RACADM et SMCLP. Pour plus d'informations sur l'interface RACADM, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **support.dell.com/manuals**. Pour plus d'informations sur SMCLP, voir Utilisation de SMCLP. **REMARQUE :** Telnet n'est pas un protocole sécurisé et il est désactivé par défaut. Telnet transmet toutes les données, y compris les mots de passe en texte clair. Pour transmettre des données sensibles utilisez l'interface SSH
SSH	Utilisez SSH pour exécuter des commandes RACADM et SMCLP. SSH fournit les mêmes fonctions que la console Telnet en utilisant une couche de transport cryptée pour renforcer la sécurité. Le service SSH est activé par défaut sur iDRAC7. Le service SSH peut être désactivé dans iDRAC7. iDRAC7 prend uniquement en charge la version SSH 2 avec DSA et l'algorithme de clé d' hôte de 1 024 bits. Une clé d'hôte unique DSA de 1 024 bits et RSA de 1 024 bits est générée lorsque vous démarrez iDRAC7 pour la première fois.
IPMItool	Utilisez l'outil IPMITool pour accéder aux fonctions de gestion de base du système distant via iDRAC7. L'interface inclut l'interface IPMI locale, IPMI sur LAN, IPMI sur série et Série sur LAN. Pour plus d'informations sur IPMITool, voir le *Guide d'utilisation des utilitaires de contrôleur de gestion Dell OpenManage Baseboard* (Dell OpenManage Baseboard Management Controller Utilities User's Guide) à l'adresse **dell.com/support/manuals**.
VMCLI	Utilisez l'interface VMCLI (Virtual Media Command Line Interface) pour accéder à un support distant via la station de gestion et déployer des systèmes d'exploitation sur plusieurs systèmes gérés.
SMCLP	Utilisez le protocole SMCLP (Server Management Workgroup Server Management-Command Line Protocol) pour exécuter des tâches de gestion de systèmes. Il est disponible via SSH ou Telnet. Pour plus d'informations sur SMCLP, voir Utilisation de SMCLP.
WS-MAN	LC-Remote Services repose sur le protocole de gestion WS pour exécuter des tâches de gestion de systèmes un à plusieurs. Vous devez utiliser un client WS-MAN, tel que WinRM (Windows) ou le client OpenWSMAN (Linux), pour pouvoir utiliser la fonctionnalité LC-Remote Services. Vous pouvez également utiliser Power Shell et Python pour exécuter des scripts vers l'interface WS-MAN. Web Services for Management (WS-Management) est un protocole SOAP (Simple Object Access Protocol) qui permet de gérer les systèmes. iDRAC7 utilise WS–Management pour transporter les informations de gestion CIM (Common Information Model) DMTF (Distributed Management Task Force). Les informations CIM définissent la sémantique et les types d'informations qui peuvent être modifiés dans un système géré. Les données disponibles vis

Interface ou protocole	Description
	WS-Management sont fournies par l'interface d'instrumentation iDRAC7 mappée vers les profils DMTF et les profils d'extension. Pour plus d'informations, consultez : • le Guide d'utilisation du Lifecycle Controller-Services à distance disponible à l'adresse **dell.com/support/manuals**. • le Guide des meilleures pratiques d'intégration du Lifecycle Controller disponible à l'adresse **dell.com/support/manuals** • la page Lifecycle Controller sur le site Dell TechCenter : **delltechcenter.com/page/Lifecycle+Controller** • Lifecycle Controller WS-Management Script Center — **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller.** • fichiers MOF et profils : **delltechcenter.com/page/DCIM.Library** • site Web DTMF : **dmtf.org/standards/profiles/**

Informations sur les ports iDRAC7

Les ports suivants sont requis pour accéder à distance à iDRAC7 à travers les pare-feux. Il s'agit des ports par défaut qu'iDRAC7 écoute pour les connexions. Facultativement, vous pouvez modifier la plupart des ports. Pour ce faire, voir Configuration des services.

Tableau 4. Ports qu'écoute iDRAC7 pour les connexions

Numéro de port	Fonction
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
161*	SNMP
5900*	Redirection du clavier et de la souris de la console, média virtuel, dossiers virtuels et partage de fichier distant
5901	VNC Lorsque la fonctionnalité VNC est activée, le port 5901 s'ouvre.

* Port configurable

La liste suivante répertorie les ports qu'iDRAC7 utilise comme client.

Tableau 5. Ports qu'iDRAC7 utilise comme client

Numéro de port	Fonction
25*	SMTP
53	DNS
68	Adresse IP attribuée par DHCP
69	TFTP
162*	Interruption SNMP

Numéro de port	Fonction
445	CIFS (Common Internet File System)
636	LDAPS (LDAP Over SSL)
2049	NFS (Network File System)
123	Protocole de temps de réseau (NTP)
3 269	LDAPS pour le catalogue global (CG)

* Port configurable

Autres documents utiles

Outre le présent guide, les documents suivants disponibles sur le site Web du support de Dell à l'adresse **dell.com/support/manuals** fournissent des informations supplémentaires sur la configuration et le fonctionnement d'iDRAC7 au sein de votre système.

- L'*Aide en ligne d'iDRAC7* fournit des informations détaillées sur les champs disponibles dans l'interface Web d'iDRAC7 et leur description. Vous pouvez accéder à l'aide en ligne après avoir installé iDRAC7.
- Le *Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC* fournit des informations sur les sous-commandes RACADM, les interfaces prises en charge, les groupes de bases de données des propriétés iDRAC7 et les définitions d'objets.
- Le *Guide de présentation de Systems Management* fournit des informations sur les logiciels disponibles pour exécuter des tâches de gestion de systèmes.
- Le *Dell Lifecycle Controller User's Guide* (Guide d'utilisation Dell Lifecycle Controller) fournit des informations sur l'utilisation de l'interface utilisateur graphique (GUI) du Lifecycle Controller.
- Le *Dell Lifecycle Controller Remote Services Quick Start Guide* (Guide de démarrage rapide des services distants Dell Lifecycle Controller) présente les capacités des services distants, fournit des informations sur la mise en route des services distants et de l'interface API Lifecycle Controller et fournit des références pour les différentes ressources du Centre technologique Dell.
- Le *Dell Remote Access Configuration Tool User's Guide* (Guide d'utilisation de l'outil de configuration de l'accès à distance Dell) explique comment utiliser l'outil de détection des adresses IP iDRAC dans le réseau et comment exécuter des mises à jour de micrologiciel un à plusieurs et des configurations Active Directory pour les adresses IP découvertes.
- Le document *Matrice de prise en charge logicielle des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- Le *Guide d'installation du module de service iDRAC* fournit des informations pour installer le module de service iDRAC.
- Le *Guide d'installation de Dell OpenManage Server Administrator* contient les instructions d'installation de Dell OpenManage Server Administrator.
- Le *Guide d'installation de Dell OpenManage Management Station Software* contient les instructions d'installation du logiciel de station de gestion Dell OpenManage qui inclut l'utilitaire de gestion de la carte mère, les outils DRAC et le snap-in d'Active Directory.
- Le *Guide d'utilisation des utilitaires de gestion des contrôleurs Dell OpenManage Baseboard Management* contient des informations sur l'interface IPMI.
- Les *Notes de mise à jour* fournissent des mises à jour de dernière minute du système ou de la documentation ou encore des informations techniques avancées destinées aux utilisateurs expérimentés ou aux techniciens.
- Le *Glossaire* fournit des informations sur les termes utilisés dans ce document.

Les documents suivants sur les systèmes sont disponibles. Ils fournissent des informations complémentaires :

- Le *Guide de présentation et des fonctions iDRAC7* fournit des informations sur iDRAC7, ses fonctions disponibles sous licence et les options de mise à niveau des licences.

- Les instructions de sécurité fournies avec votre système contiennent d'importantes instructions de sécurité et réglementaires. Pour plus d'informations réglementaires, voir la page d'accueil Regulatory Compliance sur le site Web **dell.com/regulatory_compliance**. Des informations de garantie peuvent être incluses dans ce document ou dans un document distinct.
- Les *instructions d'installation en rack*, fournies avec le rack, expliquent comment installer le système en rack.
- Le *Guide de mise en route* présente les fonctionnalités du système, les procédures de configuration et les caractéristiques techniques.
- Le *Manuel du propriétaire* contient des informations sur les caractéristiques du système, ainsi que des instructions relatives au dépannage et à l'installation ou au remplacement de composants du système.

Liens connexes

Contacter Dell

Accès aux documents à partir du site de support Dell

Référence des médias sociaux

Pour en savoir plus sur ce produit et les meilleures pratiques et pour avoir des informations concernant les services et les solutions Dell, accédez aux plateformes des médias sociaux, telles que Dell TechCenter. Accédez aux blogues, forums, livres blancs, présentations vidéos, etc. depuis la page wiki d'iDRAC à l'adresse **www.delltechcenter.com/idrac**.

Pour consulter des documents concernant iDRAC ou d'autres micrologiciels associés, voir **www.dell.com/esmmanuals**.

Contacter Dell

REMARQUE : Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le borderau de colisage, la facture le catalogue des produits Dell.

Dell propose diverses options d'assistance et de maintenance en ligne et téléphonique. Ces options varient en fonction du pays et du produit et certains services peuvent ne pas être disponibles dans votre région Pour contacter le service commercial, technique ou client de Dell :

1. Consultez le site **dell.com/support**.
2. Sélectionnez la catégorie d'assistance.
3. Vérifiez votre pays ou région dans le menu déroulant Pays/Région situé en haut de la page.
4. Sélectionnez le lien de service ou d'assistance approprié.

Accès aux documents à partir du site de support Dell

Pour accéder aux documents à partir du site de support Dell :

1. Rendez-vous sur **dell.com/support/manuals**.
2. Dans la section **Parlez-nous de votre système Dell**, sous **Non**, sélectionnez **Choisissez parmi une liste de tous les produits Dell** et cliquez sur **Continuer**.
3. Dans la section **Sélectionnez votre type de produit**, cliquez sur **Logiciel et sécurité**.
4. Dans la section **Choisissez votre logiciel Dell**, cliquez sur le lien nécessaire parmi les liens suivants :
   - **Client System Management**
   - **Enterprise System Management**
   - **Remote Enterprise System Management**
   - **Serviceability Tools**
5. Pour afficher le document, cliquez sur la version de produit nécessaire.

REMARQUE : Vous pouvez également accéder directement aux documents à l'aide des liens suivants :

- Pour les documents Enterprise System Management : **dell.com/openmanagemanuals**
- Pour les documents Remote Enterprise System Management : **dell.com/esmmanuals**
- Pour les documents Serviceability Tools : **dell.com/serviceabilitytools**
- Pour les documents Client System Management : **dell.com/OMConnectionsClient**
- Pour les documents de gestion des systèmes OpenManage Connections Enterprise : **dell.com/OMConnectionsEnterpriseSystemsManagement**
- Pour les documents de gestion des systèmes OpenManage Connections Client : **dell.com/OMConnectionsClient**

2

Ouverture de session dans iDRAC7

Vous pouvez ouvrir une session dans iDRAC7 comme utilisateur iDRAC7, utilisateur Microsoft Active Directory ou utilisateur LDAP. Le nom d'utilisateur et le mot de passe par défaut sont respectivement root et calvin. Vous pouvez également ouvrir la session en utilisant la connexion directe (SSO) ou une carte à puce.

REMARQUE : Vous devez disposer du privilège de connexion à iDRAC pour pouvoir ouvrir une session dans iDRAC7.

Liens connexes

Ouverture de session dans iDRAC7 comme utilisateur local, utilisateur Active Directory ou utilisateur LDAP
Ouverture de session dans iDRAC7 à l'aide de la carte à puce
Ouverture d'une session iDRAC7 en utilisant le connexion directe
Modification du mot de passe d'ouverture de session par défaut

Ouverture de session dans iDRAC7 comme utilisateur local, utilisateur Active Directory ou utilisateur LDAP

Avant de vous connecter à iDRAC7 avec l'interface Web, vérifiez que vous avez configuré un navigateur Web pris en charge et que le compte utilisateur a été créé avec les privilèges nécessaires.

REMARQUE : Le nom d'utilisateur Active Directory *ne tient pas compte* de la casse. Le mot de passe tient compte de la casse pour tous les utilisateurs.

REMARQUE : Outre Active Directory, les services d'annuaire openLDAP, openDS, Novell eDir et Fedora sont pris en charge. Les caractères « < » et « > » ne sont pas autorisés dans le nom d'utilisateur.

Pour ouvrir une session dans iDRAC7 comme utilisateur local, utilisateur Active Directory ou utilisateur LDAP :

1. Ouvrez un navigateur Web pris en charge.
2. Dans le champ **Adresse**, tapez `https://[adresse IP iDRAC7]` et appuyez sur <Entrée>.

   REMARQUE : Si le numéro de port HTTPS par défaut (443) a été changé, entrez `https://[adresse IP iDRAC7]:[numéro de port]`, où `[adresse IP iDRAC7]` est l'adresse IPv4 ou IPv6 d'iDRAC7 et `[numéro de port]` est le numéro de port HTTPS.

   La page d'**ouverture de session** s'affiche.
3. Pour un utilisateur local :
   - Dans les champs de **nom d'utilisateur** et de **mot de passe**, entrez votre nom d'utilisateur et votre mot de passe iDRAC7.
   - Dans le menu déroulant **Domaine**, sélectionnez **Cet iDRAC**.

4. Pour un utilisateur Active Directory, dans les champs de **nom d'utilisateur** et de **mot de passe**, entrez le nom d'utilisateur et le mot de passe Active Directory. Si vous avez spécifié le nom de domaine dans le nom d'utilisateur, sélectionnez **Cet iDRAC** dans le menu déroulant. Le format du nom d'utilisateur peut être <domaine>\<nom d'utilisateur>, <domaine>/<nom d'utilisateur> ou <utilisateur>@<domaine>.

   Par exemple, dell.com\jean_douart ou JEAN_DOUART@DELL.COM.

   Si le domaine n'est pas défini dans le nom d'utilisateur, sélectionnez le domaine Active Directory dans le menu déroulant **Domaine**.
5. Pour un utilisateur LDAP, dans les champs de **nom d'utilisateur** et de **mot de passe**, entrez votre nom d'utilisateur et votre mot de passe LDAP. Le nom de domaine n'est pas nécessaire pour la connexion LDAP. Par défaut, **Cet iDRAC** est sélectionné dans le menu déroulant.
6. Cliquez sur **Envoyer**. Vous avez ouvert une session dans iDRAC7 avec les privilèges nécessaires.

   Si vous ouvrez une session avec des privilèges de configuration d'utilisateurs et les coordonnées de compte par défaut, et si la fonction d'avertissement de mot de passe par défaut est activée, la page **Avertissement de mot de passe** s'affiche, vous permettant de modifier facilement le mot de passe.

Liens connexes

Configuration des comptes et des privilèges des utilisateurs
Modification du mot de passe d'ouverture de session par défaut
Configuration des navigateurs Web compatibles

Ouverture de session dans iDRAC7 à l'aide de la carte à puce

Vous pouvez vous ouvrir une session dans iDRAC7 en utilisant une carte à puce. Les cartes à puce fournissent une authentification bifactorielle (TFA) qui fournit une double sécurité :

- Périphérique de carte à puce physique.
- Code secret, tel qu'un mot de passe ou un code PIN.

Les utilisateurs doivent vérifier leurs données d'identification à l'aide de la carte à puce et du code PIN.

Liens connexes

Ouverture de session dans iDRAC7 en tant qu'utilisateur local à l'aide d'une carte à puce
Ouverture de session dans iDRAC7 comme utilisateur Active Directory par carte à puce

Ouverture de session dans iDRAC7 en tant qu'utilisateur local à l'aide d'une carte à puce

Avant de vous connecter comme utilisateur local en utilisant une carte à puce :

- Téléversez le certificat d'utilisateur de carte à puce et le certificat d'autorité de certification de confiance vers iDRAC7
- Activez l'ouverture de session par carte à puce.

L'interface Web d'iDRAC7 affiche la page d'ouverture de session par carte à puce pour les utilisateurs qui sont configurés pour utiliser une carte à puce.

REMARQUE : Selon les paramètres de votre navigateur, un message peut vous inviter à télécharger et installer le plug-in ActiveX lorsque vous utilisez cette fonction pour la première fois.

Pour vous connecter à iDRAC7 comme utilisateur local à l'aide d'une carte à puce :

1. Accédez à l'interface Web d'iDRAC7 en utilisant le lien `https://[Adresse IP]`.
   La page **Ouverture de session iDRAC7** qui apparaît vous invite à insérer la carte à puce.

   REMARQUE : Si le numéro de port HTTPS par défaut 443 a été changé, tapez `https://[Adresse IP]:[numéro de port]`, où `[Adresse IP]` est l'adresse IP d'iDRAC7 et `[numéro de port]` le numéro de port HTTPS.
2. Insérez la carte à puce dans le lecteur et cliquez sur **Ouvrir une session**.
   Une invite demande le code PIN de la carte. Aucun mot de passe n'est nécessaire.
3. Entrez le code PIN de la carte pour les utilisateurs de carte à puce locaux.
   Vous avez ouvert une session sur iDRAC7.

   REMARQUE : Si vous êtes un utilisateur local et que l'option **Activer la vérification d'ouverture de session par carte à puce** est activée, iDRAC7 tente de télécharger la liste de révocation de certificats et recherche, dans la liste, le certificat de l'utilisateur. La connexion échoue si le certificat est indiqué comme étant révoqué dans la liste ou s'il est impossible de télécharger la liste pour une quelconque raison.

Liens connexes

Activation ou désactivation da l'ouverture de session par carte à puce
Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs locaux

Ouverture de session dans iDRAC7 comme utilisateur Active Directory par carte à puce

Avant de vous connecter comme utilisateur Active Directory en utilisant une carte à puce :

- Téléversez un certificat d'autorité de certification de confiance (CA) (certificat Active Directory signépar une autorité de certification) vers iDRAC7.
- Configurez le serveur DNS.
- Activez la connexion Active Directory.
- Activez l'ouverture de session par carte à puce

Pour vous connecter à iDRAC7 comme utilisateur Active Directory en utilisant une carte à puce

1. Connectez-vous à iDRAC7 en utilisant le lien `https://[adresse IP]`.
   La page de **connexion iDRAC7** apparaît et vous invite à insérer la carte à puce.

   REMARQUE : Si le numéro de port HTTPS par défaut (443) est modifié, tapez `https://[adresse IP]:[numéro de port]`, où `[adresse IP]` est l'adresse IP iDRAC7 et `[numéro de port]` est le numéro de port HTTPS.
2. Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.
   La fenêtre contextuelle du **code PIN** s'affiche.
3. Saisissez le code NIP, puis cliquez sur **Submit** (Envoyer).
   Vous êtes connecté à iDRAC7 avec les données d'identification Active Directory.

   REMARQUE :

   Si l'utilisateur de la carte à puce est présent dans Active Directory, aucun mot de passe Active Directory n'est nécessaire.

Liens connexes

Activation ou désactivation da l'ouverture de session par carte à puce

Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs Active Directory

Ouverture d'une session iDRAC7 en utilisant le connexion directe

Lorsque la connexion unique (SSO) est activée, vous pouvez ouvrir une session dans iDRAC7 sans entrer vos données d'identification d'utilisateur de domaine, telles que le nom d'utilisateur et le mot de passe.

Liens connexes

Configuration d'ouverture de session par connexion directe (SSO) iDRAC7 pour les utilisateurs Active Directory

Ouverture d'une session dans iDRAC7 par la connexion directe iDRAC7 en utilisant l'interface Web d'iDRAC7

Avant de vous connecter à iDRAC7 en utilisant la connexion directe vérifiez que :

- Vous vous êtes connecté au système en utilisant un compte utilisateur Active Directory.
- L'option de connexion directe est activée pendant la configuration Active Directory.

Pour ouvrir une session dans iDRAC7 en utilisant l'interface Web :

1. Ouvrez une session sur poste de gestion en utilisant un compte Active Directory.
2. Dans un navigateur Web, tapez `https://[Adresse nom domaine complet qualifié]`

   REMARQUE : Si le numéro de port HTTPS par défaut (443) a été changé, tapez `https://[adresse nom domaine complet qualifié]:[numéro de port]`, où `[adresse nom domaine complet qualifié]` est le nom de domaine complet qualifié iDRAC7 (iDRAC7nomdns.nom.domaine) et `[numéro de port]` est le numéro de port HTTPS.

   REMARQUE : Si vous utilisez une adresse IP au lieu d'un nom de domaine complet qualifié, la connexion directe échoue.

   iDRAC7 vous connecte avec les privilèges Microsoft Active Directory appropriés en utilisant vos données d'identification mises en cache dans le système d'exploitation lorsque vous vous êtes connecté en utilisant un compte Active Directory.

Ouverture d'une session dans iDRAC7 par la connexion directe en utilisant l'interface Web CMC

La fonction de connexion directe (SSO) permet de lancer l'interface Web d'iDRAC7 depuis l'interface Web CMC. Un utilisateur CMC dispose des privilèges CMC lorsqu'il lance iDRAC7 depuis CMC.Si le compte d'utilisateur est présent dans CMC, mais pas dans iDRAC, l'utilisateur peut toujours lancer iDRAC7 depuis CMC.

Si le LAN réseau iDRAC7 est désactivé (LAN activé = non), la connexion directe n'est pas disponible.

Si le serveur est supprimé du châssis, l'adresse IP d'iDRAC7 est modifiée ou qu'il existe un problème de connexion réseau iDRAC7, l'option de lancement d'iDRAC7 est désactivée dans l'interface Web CMC.

Pour plus d'informations, voir le *Chassis Management Controller User's Guide* (Guide d'utilisation de Chassis Management Controller) disponible à l'adresse **dell.com/support/manuals**.

Accès à iDRAC7 à l'aide de l'interface RACADM

Vous pouvez utiliser l'interface distante RACADM pour accéder à iDRAC7 en utilisant l'utilitaire RACADM.

Pour plus d'informations, voir le *RACADM Reference Guide for iDRAC7 and CMC* (Guide de référence RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Si la station de gestion n'a pas stocké le certificat SSL d'iDRAC7 dans son emplacement de stockage des certificats par défaut, un message d'avertissement s'affiche lorsque vous exécutez la commande RACADM. Cependant la commande aboutit.

REMARQUE : Le certificat iDRAC7 est le certificat qu'iDRAC7 envoie au client RACADM pour établir la connexion sécurisée. Ce certificat est émis par une autorité de certification ou il est autosigné. Dans les deux cas, si la station de gestion ne reconnaît pas l'autorité de certification ou l'autorité signataire, un message d'avertissement s'affiche.

Liens connexes

Validation d'un certificat d'autorité de certification (CA) pour utiliser l'interface distante RACADM sur Linux

Validation d'un certificat d'autorité de certification (CA) pour utiliser l'interface distante RACADM sur Linux

Avant d'exécuter des commandes RACADM distantes, validez le certificat CA qui permet de protéger les communications.

Pour valider le certificat pour utiliser l'interface distante RACADM :

1. Convertissez le certificat de format DER dans le format PEM (en utilisant l'outil de ligne de commande openssl) :
   ```
   openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem -out [outcertfileinpemformat.pem] -text
   ```
2. Recherchez l'emplacement du module de certificat d'autorité de certification par défaut sur la station de gestion. Par exemple, pour RHEL5 64 bits, il s'agit de **/etc/pki/tls/cert.pem**.
3. Ajoutez le certificat PEM d'autorité de certification au certificat d'autorité de certification de la station de gestion.
   Par exemple, utilisez la `commande cat : - cat testcacert.pem >> cert.pem`
4. Générez et envoyez le certificat serveur à iDRAC7.

Accès à iDRAC7 à l'aide de l'interface locale RACADM

Pour plus d'informations sur l'accès à iDRAC7 à l'aide de l'interface locale RACADM, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Accès à iDRAC7 en utilisant le micrologiciel RACADM

Vous pouvez utiliser l'interface SSH ou Telnet pour accéder à iDRAC7 et exécuter des commandes de l'interface RACADM du micrologiciel. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **support.dell.com/manuals**.

Accès à iDRAC7 en utilisant SMCLP

SMCLP est l'invite de ligne de commande par défaut lorsque vous ouvrez une session dans iDRAC7 en utilisant Telnet ou SSH. Pour plus d'informaitons, voir Utilisation de SMCLP.

Connexion à iDRAC7 à l'aide de l'authentification par clé publique

Vous pouvez vous connecter à iDRAC7 sur SSH sans entrer de mot de passe. Vous pouvez également envoyer une simple commande RACADM comme argument de ligne de commande à l'application SSH. Les options de ligne de

commande fonctionnent pratiquement comme l'interface distante RACADM du fait que la session se termine à la fin de la commande.

Par exemple :

Connexion :

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

ou

```
ssh nom d'utilisateur@<adresse_IP>
```

où `adresse_IP` correspond à l'adresse IP d'iDRAC7.

Envoi de commandes RACADM :

```
ssh nom d'utilisateur@<domaine> racadm getversion
```

```
ssh nom d'utilisateur@<domaine> racadm getsel
```

Liens connexes

Utilisation de l'authentification par clé publique pour SSH

Sessions iDRAC7 multiples

Le tableau suivant répertorie les sessions iDRAC7 multiples possibles à l'aide des diverses interfaces.

Tableau 6. Sessions iDRAC7 multiples

Interface	Nombre de sessions
Interface Web iDRAC7	4
Interface RACADM distante	4
Micrologiciel RACADM/SMCLP	SSH - 2 Telnet - 2 Série - 1

Modification du mot de passe d'ouverture de session par défaut

Le message d'avertissement qui vous permet de modifier le mot de passe par défaut s'affiche si :

- Vous vous connectez à l'iDRAC7 avec le privilège Configurer les utilisateurs.
- La fonction d'avertissement de mot de passe par défaut est activée.
- Les coordonnées de tout compte actuellement activé sont root/calvin.

Le même message d'avertissement s'affiche si vous vous connectez à l'aide de Active Directory ou LDAP. Les comptes Active Directory et LDAP ne sont pas pris en compte lorsque vous tentez de déterminer si un compte (local) possède les coordonnées root/calvin. Un message d'avertissement s'affiche également lorsque vous vous connectez à l'iDRAC à l'aide de SSH, Telnet, l'interface RACADM distante, ou de l'interface Web. Pour l'interface Web, SSH et Telnet, un message d'avertissement unique s'affiche pour chaque session. Dans le cas de l'interface RACADM distante, le message d'avertissement s'affiche pour chaque commande.

Pour modifier les coordonnées, vous devez disposer du privilège Configurer les utilisateurs.

Liens connexes

Activation ou désactivation du message d'avertissement du mot de passe par défaut

Modification du mot de passe d'ouverture de session par défaut à l'aide de l'interface Web

Lorsque vous ouvrez une session sur l'interface Web iDRAC7, si la page **Avertissement de mot de passe par défaut** s'ouvre, cela signifie que vous pouvez changer le mot de passe. Pour ce faire :

1. Sélectionnez l'option **Modifier le mot de passe par défaut**.
2. Dans le champ **Nouveau mot de passe**, saisissez le nouveau mot de passe.

   Le mot de passe peut contenir un maximum de 20 caractères. Les caractères sont masqués. Les caractères suivants sont pris en charge :

   - 0-9
   - A-Z
   - A-Z
   - Caractères spéciaux : +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, I, \
3. Dans le champ **Confirmer le mot de passe**, saisissez de nouveau le mot de passe.
4. Cliquez sur **Continuer**. Le nouveau mot de passe est configuré et votre session s'ouvre sur l'iDRAC.

   REMARQUE : Le champ **Continuer** est activé uniquement si les mots de passe saisis dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe** correspondent.

   Pour plus d'informations sur les autres champs, voir l'*Aide en ligne d'iDRAC7*.

Modification du mot de passe d'ouverture de session par défaut à l'aide de RACADM

Pour modifier le mot de passe, exécutez la commande RACADM suivante :

```
racadm set iDRAC.Users.<index>.Password <mot_de_passe>
```

où, `<index>` est une valeur comprise entre 1 et 16 (correspond au compte utilisateur) et `<mot_de_passe>` est le nouveau mot de passe défini par l'utilisateur.

Pour des informations supplémentaires, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC).

Modification du mot de passe de connexion par défaut à l'aide de l'utilitaire Paramètres iDRAC

Pour modifier le mot de passe de connexion par défaut à l'aide de l'utilitaire Paramètres iDRAC :

1. Dans l'utilitaire de configuration iDRAC, accédez à **Configuration de l'utilisateur**.

   La page **Paramètres iDRAC - Configuration de l'utilisateur** s'affiche.
2. Dans le champ **Modifier le mot de passe**, saisissez le nouveau mot de passe.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

   Les informations sont enregistrées.

Activation ou désactivation du message d'avertissement du mot de passe par défaut

Vous pouvez activer ou désactiver l'affichage du message d'avertissement du mot de passe par défaut. Pour ce faire, vous devez disposer du privilège de configuration des utilisateurs.

Activation ou désactivation du message d'avertissement de mot de passe par défaut à l'aide de l'interface Web

Pour activer ou désactiver l'affichage du message d'avertissement de mot de passe par défaut suite à l'ouverture d'une session sur iDRAC :

1. Allez sous **Présentation** → **Paramètres iDRAC** → **Authentification utilisateur** → **Utilisateurs locaux**.

   La page **Utilisateurs** s'affiche.
2. Dans la section **Avertissement de mot de passe par défaut**, sélectionnez **Activer**, puis cliquez sur **Appliquer** pour activer l'affichage de la page **Avertissement de mot de passe par défaut** lorsque vous ouvrez une sessions sur iDRAC7. Sinon, sélectionnez **Désactiver**.

   En variante, si cette fonction est activée et que vous ne souhaitez pas que le message d'avertissement s'affiche pour les ouvertures de session suivantes, à la page **Avertissement de mot de passe par défaut**, sélectionnez l'option **Ne plus afficher cet avertissement**, puis cliquez sur **Appliquer**.

Activation ou désactivation du message d'avertissement pour modifier le mot de passe d'ouverture de session par défaut à l'aide de RACADM

Pour activer l'affichage du message d'avertissement pour modifier le mot de passe d'ouverture de session par défaut à l'aide de RACADM, utilisez l'objet `idrac.tuning.DefaultCredentialWarning`. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

3

Installation du système géré et de la station de gestion

Pour pouvoir exécuter la gestion de systèmes hors bande à l'aide d'iDRAC7, vous devez configurer iDRAC7 pour l'accès à distance, installer la station de gestion et le système géré et configurer les navigateurs Web compatibles.

REMARQUE : S'il s'agit de serveurs lames, installez les modules CMC et E/S dans le châssis et installez physiquement le système dans le châssis avant d'exécuter les configurations.

iDRAC Express et iDRAC Enterprise sont livrés par l'usine avec une adresse IP statique par défaut. Cependant, Dell offre également deux options de découverte automatique qui vous permettent d'accéder à l'iDRAC, puis de configurer à distance votre serveur et DHCP :

- Découverte automatique : utilisez cette option si un serveur de provisionnement est installé dans l'environnement de votre centre de données. Un serveur de provisionnement gère et automatise le déploiement ou la mise à niveau d'un système d'exploitation et des applications vers un serveur Dell PowerEdge. Lorsque vous activez la découverte automatique, les serveurs recherchent, lors du démarrage initial, le serveur de provisionnement afin d'en prendre le contrôle et d'amorcer le processus automatique de déploiement ou de mise à jour.
- DHCP : utilisez cette option si un serveur DHCP (Dynamic Host Configuration Protocol - Protocole de configuration dynamique d'hôte) est installé dans l'environnement de votre centre de données. Le serveur DHCP attribue automatiquement l'adresse IP, la passerelle et le masque sous-réseau d'iDRAC7.

Vous pouvez activer la découverte automatique ou le protocole DHCP lorsque vous commandez le serveur. Aucun frais n'est lié à l'activation de ces fonctionnalités. Une seule configuration est possible.

Liens connexes

Définition de l'adresse IP d'iDRAC7
Installation du système géré
Mise à jour du micrologiciel de périphérique
Restauration du micrologiciel du périphérique
Installation de la station de gestion
Configuration des navigateurs Web compatibles

Définition de l'adresse IP d'iDRAC7

Vous devez définir les paramètres réseau initiaux en fonction de l'infrastructure du réseau pour permettre les communications vers et depuis iDRAC7. Vous pouvez définir l'adresse IP à l'aide de l'une des interfaces suivantes :

- Utilitaire de configuration iDRAC
- Lifecycle Controller (voir le *Guide d'utilisation de Lifecycle Controller*)
- Dell Deployment Toolkit (voir le *Guide d'utilisation Dell Deployment Toolkit*)
- Panneau LCD du châssis ou du serveur (voir le *Manuel du propriétaire du matériel*) du système

  REMARQUE : S'il s'agit de serveurs lames, vous pouvez configurer les paramètres réseau à l'aide du panneau LCD du châssis uniquement au cours de la configuration initiale de CMC. Une fois le châssis déployé, vous ne pouvez pas reconfigurer iDRAC7 à l'aide du panneau LCD du châssis.
- Interface Web CMC (voir le *Guide d'utilisation de Dell Chassis Management Controller Firmware)*

S'il s'agit de serveurs en rack ou de type tour, vous pouvez définir l'adresse IP ou utiliser l'adresse IP d'iDRAC7 IP par défaut 192.168.0.120 pour définir les paramètres réseau initiaux, y compris configurer DHCP ou l'adresse IP statique pour iDRAC7.

S'il s'agit de serveurs lames, l'interface réseau d'iDRAC7 est désactivée par défaut.

Après avoir défini l'adresse IP d'iDRAC7 :

- Veillez à *changer le nom d'utilisateur et le mot de passe par défaut*.
- Accédez à l'adresse en utilisant l'une des interfaces suivantes :
  - Interface Web iDRAC7 à l'aide d'un navigateur pris en charge (Internet Explorer, Firefox, Chrome, ou Safari)
  - Secure Shell (SSH) : exige un client, tel que PuTTY sur Windows. SSH est disponible par défaut dans la plupart des systèmes Linux et il ne nécessite donc pas de client.
  - Telnet (doit être activé, car il est désactivé par défaut)
  - IPMITool (utilise la commande IPMI) ou invite de shell (nécessite le programme d'installation personnalisé Dell dans Windows ou Linux. disponible depuis le DVD *Systems Management Documentation and Tools* ou sur le site **support.dell.com**)

Liens connexes

Définition de l'adresse IP d'iDRAC en utilisant l'utilitaire de configuration d'iDRAC
Définition de l'adresse IP d'iDRAC7 en utilisant l'interface Web CMC
Activation de la découverte automatique
Configuration des serveurs et des composants du serveur à l'aide de la configuration automatique

Définition de l'adresse IP d'iDRAC en utilisant l'utilitaire de configuration d'iDRAC

Pour définir l'adresse IP d'iDRAC7 :

1. Mettez le système géré sous tension.
2. Appuyez sur <F2> pendant l'auto-test de démarrage (POST).
3. Sur la page **System Setup Main Menu** (Menu principal du système de configuration), cliquez sur **iDRAC Settings** (Paramètres iDRAC).

   La page **Paramètres iDRAC** s'affiche.
4. Cliquez sur **Réseau**.

   La page **Réseau** s'affiche.
5. Définissez les paramètres suivants :
   - Network Settings (Paramètres réseau)
   - Paramètres communs
   - Paramètres IPv4
   - Paramètres IPv6
   - Paramètres IPMI
   - Paramètres VLAN
6. Revenez dans la page **System Setup Main Menu** (Menu principal de la configuration système) et cliquez sur **Terminer**.

   Les informations réseau sont enregistrées et le système redémarre.

Liens connexes

Paramètres réseau
Paramètres communs
Paramètres IPv4

Paramètres IPv6
Paramètres IPMI
Paramètres VLAN

Paramètres réseau

Pour configurer les paramètres réseau :

REMARQUE : Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.

1. Sous **Activer le NIC**, sélectionnez l'option **Activé**.
2. Dans le menu déroulant **Sélection NIC**, sélectionnez l'un des ports suivants en fonction des exigences réseau :
   - Dédié : active le périphérique distant pour utiliser l'interface réseau dédiée sur le contrôleur RAC (Remote Access Controller). Cette interface n'est pas partagée avec le système d'exploitation hôte et elle route le trafic de gestion vers un réseau physique distinct pour le séparer du trafic d'application.

     Cette option implique que le port réseau dédié d'iDRAC achemine son trafic séparément des ports LOM ou NIC du serveur. Concernant la gestion du trafic du réseau, l'option Dedicated permet d'affecter à iDRAC une adresse IP du même sous-réseau ou d'un sous-réseau différent comparé aux adresses IP affectées à la LOM ou aux cartes NIC hôtes.

     REMARQUE : L'option est disponible uniquement sur les systèmes en rack ou de type tour avec la licence iDRAC7. Pour les lames, elle est disponible par défaut.
   - LOM1
   - LOM2
   - LOM3
   - LOM4

     REMARQUE : S'il s'agit de serveurs en rack et de type tour, deux options LOM (LOM1 et LOM2) ou quatre options LOM sont disponibles en fonction du modèle du serveur. Les serveurs lames n'utilisent pas LOM pour la communication iDRAC7.
3. Dans le menu **Réseau de basculement**, sélectionnez l'une des LOM restantes. Si un réseau est défaillant, le trafic est routé via le réseau de basculement.

   REMARQUE : Si vous avez sélectionné, **Dédié** dans le menu déroulant **Sélection NIC**, l'option est désactivée.

   Par exemple, pour router le trafic réseau iDRAC7 vers LOM2 lorsque LOM1 est arrêté, sélectionnez **LOM1** pour **Sélection NIC** et **LOM2** pour **Réseau de basculement**.
4. Sous **Négociation automatique**, sélectionnez **Activé** si iDRAC7 doit définir automatiquement le mode duplex et la vitesse du réseau. Cette option est disponible uniquement pour le mode dédié. Si elle est activée, iDRAC7 définit la vitesse de réseau 10, 100 ou 1 000 Mbps en fonction de la vitesse du réseau.
5. Sous **Réseau Vitesse**, sélectionnez 10 Mbps ou 100 Mbps.

   REMARQUE : Vous ne pouvez pas définir manuellement la vitesse de réseau 1 000 Mbps. Cette option est disponible uniquement si l'option de **négociation automatique** est activée.
6. Sous **Mode duplex**, sélectionnez l'option **Semi duplex** ou **Duplex intégral**.

   REMARQUE : Si vous activez la **négociation automatique**, cette option n'est pas activée.

Paramètres communs

Si l'infrastructure réseau contient un serveur DNS, enregistrez iDRAC7 dans le DNS. Il s'agit des paramètres initiaux nécessaires aux fonctions avancées, telles que les services d'annuaires : Active Directory ou LDAP, Connexion directe et carte à puce.

Pour enregistrer iDRAC7 :

1. Sélectionnez **Enregistrer le DRAC auprès du DNS**
2. Entrez le **nom DRC DNS**.
3. Sélectionnez **Auto Config Domain Name** (Définir automatiquement le nom de domaine) pour obtenir automatiquement le nom de domaine de DHCP. Ou bien, fournissez le **nom de domaine DNS**.

Paramètres IPv4

Pour configurer les paramètres IPv4 :

1. Sélectionnez l'option **Activé** sous **Activer IPv4**.
2. Sélectionnez l'option **Activé** sous **Activer DHCP** pour que DHCP puisse affecter automatiquement une adresse IP, une passerelle et un masque de sous-réseau à iDRAC7. Sinon, sélectionnez **Désactivé** et entrer les valeurs suivantes :
   - Adresse IP statique
   - Passerelle statique
   - Masque de sous-réseau statique
3. Vous pouvez facultativement activer **Utiliser DHCP pour obtenir l'adresse du serveur DNS** pour que le serveur DHCP puisse affecter le **serveur DNS statique préféré** et le **serveur DNS statique secondaire**. Sinon, entrez les adresses IP du **serveur DNS statique préféré** et du **serveur DNS statique secondaire**.

Paramètres IPv6

En fonction de la configuration de l'infrastructure, vous pouvez également utiliser le protocole IPv6.

Pour configurer les paramètres iPv6 :

1. Sélectionnez l'option **Activé** sous **Activer IPv6**.
2. Pour que le serveur DHCPv6 affecte automatiquement l'adresse IP, la passerelle et le masque de sous-réseau à iDRAC7, sélectionnez l'option **Activé** sous **Activer la configuration automatique**. Si la fonction est activée, les valeurs statiques sont désactivées. Autrement, passez à l'étape suivante pour effectuer la configuration à l'aide de l'adresse IP statique.
3. Dans la zone **Adresse IP statique 1**, entrez l'adresse IPv6 statique.
4. Dans la zone **Longueur de préfixe statique**, entrez une valeur comprise entre 0 et128.
5. Dans la zone **Passerelle statique**, entrez l'adresse de la passerelle.
6. Si vous utilisez DHCP, activez **DHCPv6 pour obtenir les adresses des serveurs DNS** pour obtenir les adresses des serveurs DNS principal et secondaire du serveur DHCPv6. Sinon, sélectionnez **Désactivé** et procédez comme suit :
   - Dans la zone **Serveur DNS statique préféré**, entrez l'adresse IPv6 statique du serveur DNS.
   - Dans la zone **Serveur DNS statique secondaire**, entrez le serveur DNS secondaire statique.

Paramètres IPMI

Pour activer les paramètres IPMI :

1. Sous **Enable IPMI Over LAN** (Activer IPMI sur LAN), sélectionnez **Activé**.
2. Sous **Channel Privilege Limit** (Limite de privilège de canal), sélectionnez **Administrateur**, **Opérateur** ou **Utilisateur**.
3. Dans la zone **Encryption Key** (Clé de cryptage), entrez la clé de cryptage en utilisant entre 0 et 40 caractères hexadécimaux (sans espaces). Par défaut, la valeur correspond à des zéros.

Paramètres VLAN

Vous pouvez configurer iDRAC7 dans l'infrastructure VLAN. Pour définir les paramètres VLAN :

1. Sous **Enable VLAN ID** (Activer l'ID VLAN), sélectionnez **Activé**.
2. Dans la zone **VLAN ID** (ID VLAN), entrez un nombre compris entre 1 et 4 094.
3. Dans la zone **Priorité**, entrez un nombre compris entre 0 et 7 pour définir la priorité de l'ID VLAN.

Définition de l'adresse IP d'iDRAC7 en utilisant l'interface Web CMC

Pour définir l'adresse IP d'iDRAC7 en utilisant l'interface Web :

REMARQUE : Vous devez disposer du privilège Administrateur et configuration de châssis pour pouvoir définir les paramètres réseau iDRAC7 depuis CMC.

1. Ouvrez une session dans l'interface Web CMC.
2. Accédez à **Server Overview** → **Setup** → **iDRAC** (Présentation du serveur, Configurer, iDRAC).

   La page **Déployer iDRAC** s'affiche.
3. Sous **Paramètres réseau iDRAC**, sélectionnez **Activer LAN** et les autres paramètres réseau en fonction des besoins. Pour plus d'informations, voir l'*aide en ligne de CMC*.
4. Pour d'autres paramètres réseau spécifiques de chaque serveur lame, accédez à **Présentation du serveur** → **<nom serveur>**.

   La page **Condition du serveur** s'affiche.
5. Cliquez sur **Lancer iDRAC** et accédez à **Présentation** → **Paramètres iDRAC** → **Réseau**.
6. Dans la page **Réseau**, définissez les paramètres réseau suivants :
   - Paramètres réseau
   - Paramètres communs
   - Paramètres IPv4
   - Paramètres IPv6
   - Paramètres IPMI
   - Paramètres VLAN

   REMARQUE : Reportez-vous à l'*aide en ligne d'IDRAC 7* pour plus d'informations.
7. Pour enregistrer les informations réseau, cliquez sur **Appliquer**.

   Pour plus d'informations, voir le *Chassis Management Controller User's Guide* (Guide d'utilisation de Chassis Management Controller) disponible à l'adresse **dell.com/support/manuals**.

Activation de la découverte automatique

La fonction de découverte automatique permet aux serveurs nouvellement installés de détecter automatiquement la console de gestion distante qui héberge le serveur d'approvisionnement. Le *serveur d'approvisionnement* fournit des références d'utilisateur administratif personnalisées à iDRAC7 afin de pouvoir détecter et gérer les serveurs non approvisionnés depuis la console de gestion. Pour plus d'informations sur la découverte automatique, voir le *Lifecycle Controller Remote Services User's Guide* (Guide d'utilisation des services à distance Lifecycle Controller) disponible sur le site **dell.com/support/manuals**.

La découverte automatique fonctionne avec une adresse IP statique. DHCP, le serveur DNS ou le nom d'hôte DNS par défaut découvre le serveur d'approvisionnement. Si DNS est spécifié, l'adresse IP du serveur d'approvisionnement est extraite de DNS et les paramètres DHCP ne sont pas nécessaires. Si le serveur d'approvisionnement est spécifié, la découverte est ignorée et ni DHCP ni DNS ne sont nécessaires.

Vous pouvez activer la découverte automatique en utilisant l'utilitaire Paramètres iDRAC7 ou le Lifecycle Controller. Pour plus d'informations sur le Lifecycle Controller, voir le *Lifecycle Controller User's Guide* (Guide d'utilisation de Lifecycle Controller) disponible sur le site **dell.com/support/manuals**.

Si la fonction de découverte automatique n'est pas activée sur un système provenant de l'usine, le compte administrateur par défaut (avec root comme nom d'utilisateur et calvin comme mot de passe) est activé. Avant d'activer la découverte automatique, assurez-vous de désactiver ce compte administrateur. Si la découverte automatique est activée dans le Lifecycle Controller, tous les comptes utilisateur iDRAC sont désactivés jusqu'à ce que le serveur d'approvisionnement soit *découvert*.

Pour activer la découverte automatique en utilisant l'utilitaire de configuration d'iDRAC :

1. Mettez le système sous tension.
2. Au cours du test POST, appuyez sur <F2 > et accédez à **iDRAC Settings** → **Remote Enablement** (Paramètres iDRAC, Activation à distance).

   La page **iDRAC Settings Remote Enablement** (Activation à distance des paramètres iDRAC) s'affiche.
3. Activez la découverte automatique, entrez l'adresse IP du serveur d'approvisionnement et cliquez sur **Retour**.

   REMARQUE : La définition de l'adresse IP du serveur d'approvisionnement est facultative. Si vous ne la définissez pas, elle est découverte en utilisant les paramètres DHCP ou DNS (étape 7).
4. Cliquez sur **Réseau**.

   La page **iDRAC Settings Network** (Paramètres réseau iDRAC) s'affiche.
5. Activer la carte NIC.
6. Activer IPv4

   REMARQUE : IPv6 n'est pas pris en charge pour la découverte automatique.
7. Activez DHCP et obtenez le nom de domaine, l'adresse du serveur DNS et le nom de domaine DNS depuis DHCP.

   REMARQUE : L'étape 7 est facultative si l'adresse IP du serveur d'approvisionnement (étape 3) est fournie.

Configuration des serveurs et des composants du serveur à l'aide de la configuration automatique

La fonction Auto Config vous permet de configurer et d'effectuer le provisionnement de tous les composants d'un serveur (par exemple, RAID, PERC et iDRAC7) en une seule opération en important automatiquement un fichier de configuration XML. Tous les paramètres configurables sont spécifiés dans le fichier XML. Le serveur DHCP qui attribue l'adresse IP contient également les détails du fichier XML pour configurer l'iDRAC7.

Vous pouvez créer le fichier XML selon le numéro de service des serveurs ou créer un fichier XML générique que vous pouvez utiliser pour configurer tous les iDRAC7 desservis par le serveur DHCP. Ce fichier XML est stocké à un emplacement partagé (CIFS ou NFS) accessible au serveur DHCP et aux iDRAC du serveur en configuration. Le serveur DHCP utilise une option de serveur DHCP pour spécifier le nom du fichier XML, l'emplacement du fichier XML et les références utilisateur permettant d'accéder à l'emplacement du fichier.

Lorsque le contrôleur iDRAC ou CMC obtient une adresse IP auprès du serveur DHCP, le fichier XML est utilisé pour configurer les périphériques. La configuration automatique est invoquée uniquement après que l'iDRAC7 obtient son adresse IP à partir du serveur DHCP. S'il n'obtient pas de réponse ou d'adresse IP auprès du serveur DHCP, alors la configuration automatique n'est pas lancée.

REMARQUE :

- Vous pouvez activer la configuration automatique uniquement si les options **DHCPv4** et **Activer IPv4** sont activées.
- Les fonctions de configuration automatique et de détection automatique sont mutuellement exclusives. Vous devez désactiver la détection automatique pour que la fonctionnalité Configuration automatique soit active.

Si tous les serveurs Dell PowerEdge du groupe de serveurs DHCP sont du même type et portent le même numéro de modèle, alors un seul fichier xml (**config.xml**) est requis. (Ceci est le nom du fichier XML par défaut.)

Vous pouvez configurer des serveurs individuels à l'aide de différents fichiers de configuration adressés à l'aide de noms d'hôte individuels. Dans un environnement disposant de serveurs différents avec des exigences spécifiques, vous pouvez utiliser différents noms de fichier XML pour distinguer chaque serveur. Par exemple, s'il existe deux serveurs, un PowerEdge R720 et un PowerEdge R520, vous devez utiliser deux fichiers XML, **R720-config.xml** et **R520-config.xml**.

L'agent de configuration de serveur utilise les règles de la séquence suivante pour déterminer les fichiers XML du partage de fichiers à appliquer pour chaque serveur iDRAC/PowerEdge :

1. le nom de fichier spécifié en option DHCP 60.
2. **<ServiceTag>-config.xml** - Si un nom de fichier n'est pas spécifié dans l'option DHCP 60, utilisez le numéro de série du système pour identifier de manière unique le fichier de configuration XML pour le système. Par exemple, **<servicetag>-config.xml**
3. **<Model number>-config.xml** - Si le nom de fichier de l'option 60 n'est pas spécifié et que le fichier **<ServiceTag> -config.xml** est introuvable, utilisez le numéro de modèle du système en tant que base du nom du fichier de configuration XML à utiliser. Par exemple, **R520-config.xml**.
4. **config.xml** - Si les fichiers portant le nom de fichier de l'option 60, basés sur le numéro de service et le numéro de modèle ne sont pas disponibles, utilisez le fichier par défaut **config.xml**.

Liens connexes

Séquence de configuration automatique
Options DHCP
Activation de la configuration automatique à l'aide de l'interface Web de l'iDRAC
Activation de la configuration automatique à l'aide de RACADM

Séquence de configuration automatique

1. Créer ou modifier le fichier XML qui configure les attributs de serveurs Dell.
2. Placer le fichier XML sur un emplacement de partage accessible par le serveur DHCP et par tous les serveurs Dell qui ont une adresse IP affectée par le serveur DHCP.
3. Spécifier l'emplacement du fichier XML dans le champ de l'option 43 fournisseurs du serveur DHCP.
4. L'iDRAC dans le cadre de l'acquisition de l'adresse IP annonce l'iDRAC identifiant de classe fournisseur. (Option 60)
5. Le serveur DHCP fait correspondre la classe de fournisseur à l'option de fournisseur dans le fichier **dhcpd.conf** et envoie l'emplacement du fichier XML et le nom du fichier XML à l'iDRAC.
6. L'iDRAC traite le fichier XML et configure tous les attributs répertoriés dans le fichier

Options DHCP

DHCPv4 permet à un grand nombre de paramètres définis dans le monde entier d'être transmis aux clients DHCP. Chaque paramètre est reconnu comme option DHCP. Chaque option est identifiée par un numéro d'option, qui a une valeur d'1 octet. Les numéros d'option 0 et 255 sont réservés au remplissage et aux extrémités, respectivement. Toutes les autres valeurs sont disponibles pour la définition des options.

L'option DHCP 43 est utilisée pour envoyer des informations du serveur DHCP vers le client DHCP. L'option est définie comme une chaîne de texte. Cette chaîne de texte est définie pour contenir les valeurs du fichier XML, de l'emplacement de partage, et des informations d'identification pour accéder à l'emplacement. Par exemple :

```
option myname code 43 = text; option myname "-l 10.35.175.88://xmlfiles –f
dhcpProv.xml –u root –p calvin";
```

où, -l correspond au partage de fichiers à distance et -f est le nom de fichier dans la chaîne, ainsi que les informations d'identification pour le partage de fichiers à distance. Dans cet exemple, *root* et *calvin* sont le nom d'utilisateur et le mot de passe pour le RFS.

L'option DHCP 60 identifie et associe un client DHCP à un fournisseur particulier. Tout serveur DHCP configuré pour agir sur la base d'un ID de fournisseur du client doit avoir l'option 60 et l'option 43 configurées. Grâce aux serveurs Dell PowerEdge, l'iDRAC s'identifie lui-même avec un identifiant fournisseur : *iDRAC*. Par conséquent, vous devez ajouter une nouvelle « classe de fournisseur » et créer une « option d'étendue » qui en dépend pour le « code 60 », puis activer la nouvelle option d'étendue du serveur DHCP.

Liens connexes

Configuration de l'option 43 sur Windows
Configuration de l'option 60 sur Windows
Configuration de l'option 43 et de l'option 60 sur Linux

Configuration de l'option 43 sur Windows

Pour configurer l'option 43 sur Windows :

1. Sur le serveur DHCP, allez dans **Démarrer** → **Outils d'administration** → **DHCP** pour ouvrir l'outil d'administration de serveur DHCP.
2. Trouvez le serveur et développez tous les éléments de la section.
3. Effectuez un clic droit sur **Options d'étendue** et sélectionnez **Configurer les options**.

   La boîte de dialogue **Options d'étendue** s'affiche.
4. Faites défiler la fenêtre et sélectionnez **043 Informations spécifiques sur le fournisseur**.
5. Dans le champ **Entrée de données**, cliquez n'importe où dans la zone située sous **ASCII** et entrez l'adresse IP du serveur sur lequel se situe l'emplacement de partage, qui contient le fichier de configuration XML.

   La valeur s'affiche lorsque vous la tapez sous l'**ASCII**, mais elle apparaît également en binaire sur la gauche.
6. Cliquez sur **OK** pour enregistrer la configuration.

Configuration de l'option 60 sur Windows

Pour configurer l'option 60 sur Windows :

1. Sur le serveur DHCP, allez dans **Démarrer** → **Outils d'administration** → **DHCP** pour ouvrir l'outil d'administration de serveur DHCP.
2. Trouvez le serveur et développez ses éléments.
3. Cliquez avec le bouton droit sur **IPv4** et sélectionnez **Définir les classes de fournisseurs**.
4. Cliquez sur **Suivant**, puis saisissez les informations suivantes :
   - **Nom d'affichage** - iDRAC (lecture seule)
   - **Description** - Classe de fournisseur
   - Sous **ASCII**, cliquez et accédez à iDRAC.
5. Cliquez sur **OK**.
6. Dans la fenêtre DHCP, cliquez avec le bouton droit sur **IPv4** et choisissez **Configurer les options prédéfinies**.
7. Dans le menu déroulant **Option de classe**, sélectionnez **iDRAC** (créé à l'étape 4) et cliquez sur **Ajouter**.

8. Dans la boîte de dialogue **Type d'option**, entrez les informations suivantes :
   - **Nom** : iDRAC
   - **Type de données** : chaîne
   - **Code** : 1
   - **Description** : identifiant de classe de fournisseur Dell
9. Cliquez deux fois sur **OK** pour revenir à la fenêtre **DHCP** .
10. Développez tous les éléments situés sous le nom du serveur, effectuez un clic droit sur **Options d'étendue** et sélectionnez **Configurer les options**.
11. Cliquez sur l'onglet **Avancé**.
12. Dans le menu déroulant **Classe de fournisseur**, sélectionnez **iDRAC**. L'option 060iDRAC s'affiche dans la colonne **Options disponibles**.
13. Sélectionnez l'option **060iDRAC**.
14. Entrez la valeur de chaîne qui doit être envoyée à l'iDRAC (accompagnée d'une adresse IP standard fournie par le serveur DHCP). La valeur de chaîne permettra d'importer le fichier de configuration XML correct.

    Pour le paramètre d'option **Entrée de DONNÉES, valeur de chaîne**, utilisez un paramètre de texte où figurent les options de lettre et les valeurs suivantes :
    - Filename - **iDRAC_Config.XML** ou **iDRAC_Config <service-tag> .XML**. (-f)
    - Sharename - (-n)
    - ShareType - -s (0 = NFS, 2 = CIFS)
    - IPAddress - Adresse IP du partage de fichiers. (-i)
    - Username - Requis pour CIFS (-u)
    - Password - Obligatoire pour CIFS (-p)
    - ShutdownType - Spécifier normal ou forcé. (-d)
    - Timetowait - La valeur par défaut est 300 (-t)
    - EndHostPowerState - (-e)

Configuration de l'option 43 et de l'option 60 sur Linux

Mettez à jour le fichier **/etc/dhcpd.conf** . À l'instar de Windows, les étapes sont les suivantes :

1. Mettez de côté un bloc ou pool d'adresses que ce serveur DHCP peut allouer.
2. Définissez l'option 43 et utilisez l'identifiant de classe de fournisseur pour l'option 60.

Par exemple :

```
option myname code 43 = text; subnet 192.168.0.0 netmask 255.255.0.0 { #default
gateway option routers    192.168.0.1; option subnet-mask    255.255.255.0;
option nis-domain    "domain.org"; option domain-name    "domain.org"; option
domain-name-servers    192.168.1.1; option time-offset    -18000;    # Eastern
Standard Time #    option ntp-servers    192.168.1.1; #    option netbios-name-
servers    192.168.1.1; # --- Selects point-to-point node (default is hybrid).
Don't change this unless # -- you understand Netbios very well #    option
netbios-node-type 2; option vendor-class-identifier "iDRAC"; set vendor-string
= option vendor-class-identifier; option myname "2001::9174:9611:5c8d:e85//
xmlfiles/dhcpProv.xml -u root -p calvin"; range dynamic-bootp 192.168.0.128
192.168.0.254; default-lease-time 21600; max-lease-time 43200; # we want the
nameserver to appear at a fixed address host ns { next-server
marvin.redhat.com; hardware ethernet 12:34:56:78:AB:CD; fixed-address
207.175.42.254; } }
```

Activation de la configuration automatique à l'aide de l'interface Web de l'iDRAC

Assurez-vous que les options DHCPv4 et Activer IPv4 sont activées et que la détection automatique est désactivée.

Pour activer la configuration automatique :

1. Dans l'interface Web de l'iDRAC7, allez sur **Présentation générale** → **Paramètres iDRAC** → **Réseau**.
   La page **Réseau** s'affiche.
2. Dans la section **Configuration automatique** , sélectionnez l'une des options suivantes pour activer la **configuration automatique** :
   - **Activer une fois** : la configuration du composant ne s'effectue qu'une seule fois à l'aide du fichier XML référencé par le serveur DHCP. La configuration automatique est ensuite désactivée.
   - **Activer une fois après la réinitialisation** : après la réinitialisation de l'iDRAC7, la configuration du composant ne s'effectue qu'une seule fois à l'aide du fichier XML référencé par le serveur DHCP. La configuration automatique est ensuite désactivée.
   - **Toujours activer** : la configuration des composants (à l'aide du fichier XML) s'effectue chaque fois que l'iDRAC7 reçoit une adresse IP du serveur DHCP.

   Pour désactiver la fonctionnalité Configuration automatique, sélectionnez **Disable** (Désactiver).
3. Cliquez sur **Appliquer** pour appliquer le paramètre.

Activation de la configuration automatique à l'aide de RACADM

Pour activer la fonctionnalité Configuration automatique à l'aide de RACADM, utilisez l'objet `iDRAC.NIC.AutoConfig`. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC*.

Installation de la station de gestion

Une station de gestion est un ordinateur utilisé pour accéder aux interfaces iDRAC7 pour surveiller et gérer à distance les serveurs PowerEdge.

Pour installer la station de gestion :

1. Installez un système d'exploitation compatible. Pour plus d'informations, voir le fichier Lisez-moi.
2. Installez et configurez un navigateur Web pris en charge (Internet Explorer, Firefox, Chrome, ou Safari).
3. Installez le dernier environnement JRE (Java Runtime Environment) (nécessaire si le type de plug-in Java est utilisé pour accéder à iDRAC7 en utilisant un navigateur Web).
4. Depuis le DVD *Dell Systems Management Tools and Documentation*, installez l'interface distante RACADM et VMCLI depuis le dossier SYSMGMT. Ou bien, exécutez **Setup** sur le DVD pour installer l'interface distante RACADM par défaut et d'autres logiciels OpenManage. Pour plus d'informations sur l'interface RACADM, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RCADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.
5. Installez les éléments suivants en fonction des besoins :
   - Telnet
   - Client SSH
   - TFTP
   - Dell OpenManage Essentials

Liens connexes

Installation de l'utilitaire VMCI
Configuration des navigateurs Web compatibles

Accès à distance à iDRAC7

Pour accéder à distance à l'interface Web iDRAC7 depuis une station de gestion, veillez à ce que cette dernière soit dans le même réseau qu'iDRAC7. Par exemple :

- Serveurs lames : la station de gestion doit se trouver dans le même réseau que CMC. Pour plus d'informations sur l'isolement du réseau CMC du réseau du système géré, voir le *Chassis Management Controller User's Guide* (Guide d'utilisation du Chassis Management Controller) disponible à l'adresse **dell.com/support/manuals**.
- Serveurs en rack et type tour : affectez à la carte NIC iDRAC7 la valeur LOM1 et vérifiez que la station de gestion se trouve sur le même réseau qu'iDRAC7.

  REMARQUE : Si le système est mis à niveau vers iDRAC7 Enterprise, vous pouvez affecter à la carte NIC iDRAC7 NIC la valeur **Dédié.**

Pour accéder à la console du système géré depuis une station de gestion, utilisez la console virtuelle via l'interface Web iDRAC7.

Liens connexes

Lancement de la console virtuelle

Paramètres réseau

Installation du système géré

Si vous devez exécuter l'interface locale RACADM ou activer la capture du dernier écran de blocage, installez les éléments suivants depuis le DVD *Dell Systems Management Tools and Documentation* :

- Interface RACADM locale
- Server Administrator

Pour plus d'informations sur Server Administrator, consultez le *Dell OpenManage Server Administrator User's Guide* (Guide d'utilisation de Dell OpenManage Server Administrator) disponible à l'adresse **dell.com/support/manuals**.

Liens connexes

Modification des paramètres du compte d'administrateur local

Modification des paramètres du compte d'administrateur local

Après avoir défini l'adresse IP iDRAC7, vous pouvez modifier les paramètres du compte d'administrateur local (à savoir l'utilisateur 2) en utilisant l'utilitaire de configuration iDRAC. Pour ce faire :

1. Dans l'utilitaire de configuration iDRAC, accédez à **Configuration de l'utilisateur**.
   La page **Paramètres iDRAC - Configuration de l'utilisateur** s'affiche.
2. Définissez les informations pour le **nom d'utilisateur**, les **privilèges de l'utilisateur LAN**, les **privilèges de l'utilisateur du port série** et le **mot de passe**.
   Pour plus d'information sur les options, voir l'*aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Précédent**, **Terminer** et **Oui**.
   Les paramètres du compte d'administrateur sont définis.

Définition de l'emplacement du système géré

Vous pouvez définir les informations d'emplacement du système géré dans le centre de données à l'aide de l'interface Web d'iDRAC7 ou de l'utilitaire de configuration d'iDRAC.

Définition de l'emplacement du système géré en utilisant l'interface Web

Pour définir l'emplacement du système :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Serveur** → **Propriétés** → **Détails**.
   La page **Détails système** s'affiche.
2. Sous **Emplacement du système**, entrez les informations d'emplacement du système géré dans le centre de données.
   Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer**. Les informations d'emplacement du système sont enregistrées dans iDRAC7.

Définition de l'emplacement du système géré à l'aide de l'interface RACADM

Pour définir les informations d'emplacement du système géré, utilisez les objets du groupe `System.Location`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Définition de l'emplacement du système géré en utilisant l'utilitaire de configuration iDRAC

Pour définir les informations d'emplacement du système :

1. Dans l'utilitaire de configuration iDRAC, accédez à **Emplacement du système**.
   La page **Paramètres iDRAC - Emplacement du système** s'affiche.
2. Entrez les informations d'emplacement du système géré dans le centre de données. Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration iDRAC*.
3. Cliquez successivement sur **Précédent**, **Terminer** et **Oui**.
   Les informations sont enregistrées.

Optimisation des performances du système et de la consommation d'énergie

L'énergie requise pour refroidir un serveur peut augmenter de manière significative l'énergie totale consommée par le système. Le contrôle thermique est la gestion active du système de refroidissement via la gestion de la vitesse des ventilateurs et la gestion de l'alimentation du système qui permettent de s'assurer que le système est fiable tout en réduisant la consommation d'énergie du système, la ventilation et l'intensité acoustique du système. Vous pouvez régler les paramètres de contrôle thermique et optimiser les performances du système et les exigences de performance par watt.

Dans l'utilitaire des paramètres d'iDRAC, modifiez les paramètres suivants :

- Optimiser les performances
- Optimiser la puissance minimale
- Définir la température maximale d'évent
- Augmenter la ventilation via une compensation du ventilateur, si nécessaire

Pour ce faire :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Thermique**

   La page **Paramètres thermiques iDRAC** s'affiche.
2. Définissez les paramètres thermiques, l'option d'utilisateur et les paramètres du ventilateur.

   – **Algorithme thermique de base** : par défaut, il est défini sur **Automatique**, ce qui adresse aux paramètres du profil sélectionnés sous la page **BIOS système → Paramètres du BIOS système. Paramètres du profil système** . Vous pouvez également sélectionner un algorithme personnalisé, indépendant du profil BIOS. Les options disponibles sont les suivantes :

     * **Performances maximales (Performances optimisées)** : réduit l'impact des performances relatives à une source thermique aux dépens d'une puissance accrue du ventilateur. Lorsque la performance est critique et que le système d'exploitation atteint des températures élevées, la configuration de performance maximale offre une performance améliorée.
     * **Puissance minimale (Performance par watt optimisée)** : réduit la vitesse de réponse du ventilateur dans des environnements à températures élevées. Ceci réduit la puissance totale du système qui peut alors avoir moins d'impact sur la performance. La configuration de puissance minimale offre un équilibre entre la performance et la puissance. Il s'agit de l'algorithme thermique de base adressé au profil système relatif à la performance par watt. Il établit un équilibre entre les exigences de refroidissement des composants et les contraintes de performance et de puissance du système.

       L'impact des performances relatives à une source thermique ne définit pas les températures ambiantes des centres de données typiques (18 -30°C).

   – **Options de refroidissement** : sélectionnez l'option de refroidissement **Par défaut**, **Température maximale d'évent** ou **Décalage de la vitesse du ventilateur**.

   – **Température maximale d'évent (en C)** : permet à la vitesse du ventilateur du système d'accélérer de telle façon que la température d'évent ne dépasse pas 50 C. Cette option utilise plusieurs capteurs discrets de température d'évent avec contrôle de vitesse et gestion de la puissance afin de s'assurer que les températures maximales d'évent sont maintenues à 50 C maximum à l'arrière d'un serveur.

   – **Décalage de la vitesse du ventilateur (par défaut = Aucun)** : indique le décalage de la vitesse du ventilateur lorsqu'une marge thermique accrue est requise pour les cartes PCIe à haute puissance personnalisées ou pour réduire les températures d'évent du système pour des équipements adjacents tels que les commutateurs. Le décalage de la vitesse d'un ventilateur entraîne l'augmentation de la vitesse du ventilateur (de la valeur en % de décalage) au-delà des vitesses de base des ventilateurs calculées par l'algorithme de contrôle thermique. Par défaut, la valeur est None (Aucun). Sélectionnez :

     * **Décalage faible de la vitesse de ventilation** : ramène les vitesses des ventilateurs à une vitesse de ventilation modérée (approximativement 50%)
     * **Décalage élevé de la vitesse de ventilation** : ramène les vitesses des ventilateurs près de la vitesse maximale (approximativement 90-100 %).
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

   Les paramètres thermiques sont définis.

Configuration des navigateurs Web compatibles

iDRAC7 est pris en charge sur les navigateurs Web suivants : Internet Explorer, Mozilla Firefox, Google Chrome et Safari. Pour en savoir plus sur les versions, voir le fichier *Lisez-moi* disponible sur **dell.com/support/manuals**.

Si vous vous connectez à l'interface Web iDRAC7 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. Cette section fournit des informations sur la configuration d'Internet Explorer :

Pour configurer la navigateur Web Internet Explorer :

1. Configurez IE sur **Exécuter en tant qu'administrateur**.
2. Dans le navigateur Web, accédez à **Outils** → **Options Internet** → **Sécurité** → **Réseau local**.
3. Cliquez sur **Personnalisé le niveau**, sélectionnez **Moyen bas**, puis cliquez sur**Réinitialiser**. Cliquez sur **OK** pour confirmer. Cliquez sur **Personnaliser le niveau** pour ouvrir la boîte de dialogue.
4. Accédez à la section Contrôles ActiveX et plug-ins et définissez ce qui suit :

   REMARQUE : Les paramètres dans l'état Moyen bas dépendent de la version d'IE version.

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

   Téléchargements :

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

   Sous **Divers** :

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

   Sous **Script** :

   - Script actif : Activé
   - Autoriser les opérations de collage via un script : Activé
   - Script des applets Java : Activé
5. Accédez à **Outils** → **Options Internet** → **Avancé**.

6. Sous **Navigation** :

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

   Sous **Paramètres HTTP 1.1** :

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

   Sous **Java (Sun)** :

   - Utiliser JRE 1.6.x_yz : sélectionné (facultatif ; la version peut être différente)

   Sous **Multimédia** :

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

   Sous Sécurité :

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

   REMARQUE : Pour modifier les paramètres, il est recommandé de connaître et de comprendre les conséquences. Par exemple, si vous bloquez les fenêtres publicitaires intempestives, des parties de l'interface Web iDRAC7 peuvent ne pas fonctionner correctement.
7. Cliquez sur **Appliquer**, puis sur **OK**.
8. Cliquez sur l'onglet **Connexions**.
9. Sous **Paramètres du réseau local (LAN)**, cliquez sur **Paramètres du LAN**.
10. Si la case **Utiliser un serveur proxy** est cochée, cochez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.
11. Cliquez deux fois sur **OK**.
12. Fermez et redémarrez le navigateur pour vous assurer que toutes les modifications sont effectives.

Liens connexes

Ajout d'iDRAC7 à la liste des domaines de confiance

Lorsque vous accédez à l'interface Web d'iDRAC7, un message demande d'ajouter l'adresse IP d'iDRAC7 à la liste des domaines si l'adresse IP n'y figure pas. Une fois l'opération terminée, cliquez sur **Refresh** (Actualiser) ou lancer le navigateur Web afin d' établir une connexion à l'interface Web d'iDRAC7.

Sur certains systèmes d'exploitation, il est possible qu'Internet Explorer (IE) 8 ne demande pas d'ajouter l'adresse IP d'iDRAC7 à la liste des domaines de confiance si elle ne figure pas dans la liste.

REMARQUE : Lors de la connexion à l'interface Web d'iDRAC7 avec un certificat que le navigateur n'accepte pas, l'avertissement d'erreur de certificat du navigateur peut s'afficher une seconde fois après acceptation du premier. Il s'agit d'une procédure de sécurité normale.

Pour ajouter l'adresse IP d'iDRAC7 à la liste des domaines de confiance dans IE8, procédez comme suit :

1. Sélectionnez **Outils** → **Options Internet** → **Sécurité** → **Site de confiance** → **Sites**.
2. Entrez l'adresse IP d'iDRAC7 dans **Ajouter ce site Web à la zone**.
3. Cliquez successivement sur **Ajouter**, **OK et Fermer**.
4. Cliquez sur **OK**, puis actualisez votre navigateur.

Désactivation de la fonction de liste blanche dans Firefox

Firefox dispose d'une fonction de sécurité appelée « Liste blanche » qui requiert l'autorisation de l'utilisateur pour installer les plug-ins de chaque site qui héberge un plug-in. Si la fonction est activée, elle vous oblige à installer un visualiseur de console virtuelle pour chaque iDRAC7 que vous visitez, même si les versions de visualiseur sont identiques.

Pour désactiver la fonction de liste blanche et éviter l'installation inutile de plug-ins, procédez comme suit :

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 préférence** recherchez **xpinstall.whitelist.required** et cliquez deux fois dessus.
   Les valeurs des champs **Nom de préférence**, **État**, **Type** et **Valeur** sont mises en gras. La valeur **État** est remplacée par l'utilisateur défini et l'entrée **Valeur** est remplacée par false.
4. Dans la colonne de **Nom de préférence**, recherchez **xpinstall.enabled**.
   Vérifiez que **Valeur** est définie sur **vrai**. Si tel n'est pas le cas, cliquez deux fois sur **xpinstall.enabled** pour affecter à **Valeur** la valeur **vrai**.

Affichage des versions localisées de l'interface Web

L'interface Web d'iDRAC7 est disponible dans les langues suivantes :

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

Les identificateurs ISO entre parenthèses indiquent les variantes des langues. Pour certaines langues, il est nécessaire de redimensionner la fenêtre du navigateur en utilisant 1 024 pixels de largeur pour pouvoir afficher toutes les fonctions.

L'interface Web d'iDRAC7 fonctionne avec les claviers localisés pour les variantes de langues prises en charge. Certaines fonctions de l'interface Web d'iDRAC7, telles que la console virtuelle, peuvent nécessiter d'exécuter des opérations supplémentaires pour accéder à certaines fonctions ou lettres. Les autres claviers ne sont pas compatibles et peuvent générer des problèmes imprévus.

REMARQUE : Consultez la documentation du navigateur Web pour savoir comment configurer ou définir différentes langues et afficher les versions localisées de l'interface Web d'iDRAC7.

Mise à jour du micrologiciel de périphérique

Avec iDRAC7, vous pouvez mettre à jour les micrologiciels d'iDRAC7, du BIOS et des périphériques pris en charge via la mise à jout Lifecycle Controller, tels que :

- Lifecycle Controller
- Diagnostics
- Pack de pilotes de système d'exploitation
- Carte d'interface réseau (NIC)
- Contrôleur RAID
- Unité d'alimentation (PSU)
- Solid State Drives (SSD) PCIe

Vous devez mettre à jour le micrologiciel requis vers iDRAC. Une fois le téléversement terminé, la version du micrologiciel actuellement installée sur le périphérique et la version en cours d'application sont affichées. Si la version du micrologiciel en cours d'application est non valide, un message d'erreur s'affiche. Les mises à jour qui ne nécessitent pas un redémarrage du système prennent effet immédiatement. Les mises à jour qui nécessitent un redémarrage du système sont étagées et prévues pour s'exécuter au prochain démarrage du système. Seul un redémarrage du système est requis pour effectuer toutes les mises à jour.

Une fois le micrologiciel mis à jour, la page **Inventaire du système** affiche la version du micrologiciel mis à jour et les journaux sont enregistrés.

Les types de fichiers d'image micrologiciel sont les suivants :

- **.exe** — Dell Update Package (DUP) à base Windows
- **.d7**
- **.usc**
- **.pm**

Pour les fichiers ayant une extension **.exe**, vous devez disposer de privilèges de contrôle du système. La fonctionnalité de mise à jour à distance du micrologiciel et le Lifecycle Controller doivent être activés.

Pour les fichiers ayant une extension **.d7**, **.usc** ou **.pm**, vous devez disposer de privilèges de configuration.

Vous pouvez effectuer les mises à jour du micrologiciel à l'aide des méthodes suivantes :

- À l'aide du fichier d'image micrologiciel présent sur le système local ou le partage réseau.
- Mettez à jour le micrologiciel en vous connectant au site FTP ou à un espace de stockage réseau qui contient un catalogue des mises à jour disponibles. Vous pouvez créer des espaces de stockage personnalisés à l'aide de Repository Manager (Gestionnaire d'espaces de stockage). Pour des informations supplémentaires, voir le *Guide d'utilisation de Repository Manager*. iDRAC7 fournit automatiquement une différence entre le BIOS et le micrologiciel installé sur le serveur et l'emplacement de l'espace de stockage ou le site FTP. Toutes les mises à jour applicables contenues dans l'espace de stockage s'appliquent au système. Cette fonction est disponible avec la licence iDRAC7 Enterprise.

- Planifiez les mises à jour automatiques récurrentes du micrologiciel à l'aide du fichier catalogue du site FTP ou de l'emplacement de l'espace de stockage réseau.

Le tableau suivant indique si un redémarrage système est nécessaire ou non lors de la mise à jour du micrologiciel pour un composant spécifique.

REMARQUE : Lorsque plusieurs mises à jour de micrologiciel sont appliquées par le biais de méthodes hors bande, les mises à jour sont classées de la manière la plus efficace possible pour éviter les redémarrages du système.

Tableau 7. Mise à jour du micrologiciel – Composants pris en charge

Nom de composant	Restauration du micrologiciel pris en charge ? (Oui ou Non)	Hors bande : redémarrage du système requis ?	Intrabande : redémarrage du système requis ?	Interface utilisateur graphique du Lifecycle Controller : redémarrage requis ?
Diagnostics	Non	Non	Non	Non
Pack de pilotes du système d'exploitation	Non	Non	Non	Non
Lifecycle Controller	Non	Non	Non	Oui
BIOS	Oui	Oui	Oui	Oui
Contrôleur RAID	Oui	Oui	Oui	Oui
Fonds de panier	Oui	Oui	Oui	Oui
Enceintes	Oui	Oui	Non	Oui
Carte réseau	Oui	Oui	Oui	Oui
iDRAC	Oui	** Non	*Non	*Non
Module d'alimentation	Oui	Oui	Oui	Oui
CPLD	Non	Oui	Oui	Oui
Cartes FC	Oui	Oui	Oui	Oui
SSD PCIe	Oui	Oui	Oui	Oui

*Indique que même si un redémarrage du système n'est pas nécessaire, iDRAC doit être redémarré pour pour appliquer les mises à jour. Les communications et la surveillance d'iDRAC sont temporairement interrompues.

** Lorsque iDRAC7 est mise à jour à partir de la version 1.30.30 ou ultérieure, un redémarrage du système n'est pas nécessaire. Cependant, pour les versions de micrologiciel antérieures à l'iDRAC7 1.30.30, un redémarrage du système est requis lorsqu'elles sont appliquées à l'aide des interfaces hors bande.

Liens connexes

Téléchargement du micrologiciel de périphérique
Mise à jour du micrologiciel de périphérique unique
Mise à jour du micrologiciel via l'espace de stockage
Mise à jour du micrologiciel à l'aide de FTP
Mise à jour du micrologiciel de périphérique à l'aide de RACADM
Planification des mises à jour automatiques du micrologiciel
Mise à jour du micrologiciel en utilisant l'interface Web CMC

Mise à jour du micrologiciel en utilisant DUP
Mise à jour du micrologiel à l'aide de l'interface RACADM
Mise à jour du micrologiciel en utilisant le services à distance Lifecycle Controller

Téléchargement du micrologiciel de périphérique

Le format de fichier image que vous téléchargez dépend du mode de mise à jour :

- Interface Web d'iDRAC7 : téléchargez l'image binaire stockée dans une archive à extraction automatique. Le fichier image par défaut du micrologiciel est **firmimg.d7**.

  REMARQUE : Le même format de fichier est utilisé pour récupérer iDRAC7 à l'aide de l'interface Web CMC.
- Système géré : téléchargez le DUP (Dell Update Package) spécifique du système d'exploitation. Les extensions de fichier sont **.bin** pour les systèmes d'exploitation Linux et **.exe** pour les systèmes d'exploitation Windows.
- Lifecycle Controller : téléchargez le dernier fichier de catalogue et les derniers DUP et utilisez la fonction *Mise à jour de plate-forme* dans Lifecycle Controller pour mettre à jour le micrologiciel du périphérique. Pour plus d'informations sur la mise à jour de plate-forme, voir le *Lifecycle Controller User's Guide* (Guide d'utilisation de Lifecycle Controller) disponible sur le site Web **dell.com/support/manuals**.

Mise à niveau du micrologiciel en utilisant l'interface Web d'iDRAC7

Vous pouvez mettre à jour le micrologiciel du périphérique à l'aide des images de micrologiciel disponibles sur le système local, à partir d'un espace de stockage sur un partage réseau (CIFS ou NFS) ou à partir d'un serveur FTP.

Mise à jour du micrologiciel de périphérique unique

Avant de mettre à jour le micrologiciel à l'aide du procédé de mise à jour pour un seul périphérique, assurez-vous que vous avez téléchargé l'image du micrologiciel vers un emplacement du système local.

Pour mettre à jour le micrologiciel de périphérique à l'aide de l'interface Web iDRAC7 :

1. Allez sous **Présentation générale** → **Paramètres iDRAC** → **Mise à jour et restauration** .

   La page **Mise à jour de micrologiciel** s'affiche.
2. Sur l'onglet **Mise à jour** , sélectionnez **Local** comme **emplacement des fichiers**.
3. Cliquez sur **Parcourir**, sélectionnez le fichier image du micrologiciel pour le composant requis, puis cliquez sur **Téléverser**.
4. Une fois le téléversement terminé, la section **Détails de la mise à jour** affiche chaque fichier de micrologiciel téléversé sur iDRAC et son état.

   Si le fichier image du micrologiciel est valide et a été téléversé avec succès, la colonne **Contenu** affiche une icône à côté du nom du fichier image du micrologiciel. Développez le nom pour afficher le **Nom du périphérique** et les informations du micrologiciel **Actuelles** et **Disponibles**.
5. Sélectionnez le micrologiciel à mettre à jour, puis cliquez sur l'une des options suivantes :
   - Pour les images de micrologiciel qui ne nécessitent pas un redémarrage du système hôte, cliquez sur **Installer** (par exemple, le fichier micrologiciel iDRAC).
   - Pour les images de micrologiciel qui nécessitent un redémarrage du système hôte, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**.
   - Pour annuler la mise à jour du micrologiciel, cliquez sur **Annuler**.

   REMARQUE : Si vous avez téléversé le même fichier d'image micrologiciel plus d'une fois, seul le fichier de micrologiciel le plus récent est disponible pour la sélection. La case des fichiers d'image micrologiciel antérieurs est désactivée.

   Lorsque vous cliquez sur **Installer**, **Installer et redémarrer** ou **Installer au prochain redémarrage**, le message `Updating Job Queue` (Mise à jour de la file d'attente des tâches) s'affiche.

6. Cliquez sur **File d'attente des tâches** pour afficher la page **File d'attente des tâches**, laquelle vous permet d'afficher et de gérer les mises à jour de micrologiciel étagées ou de cliquer sur **OK** pour actualiser la page et voir l'état de la mise à jour du micrologiciel.

   REMARQUE : Si vous naviguez vers une autre page sans confirmer les mises à jour, un message d'erreur s'affiche et tout le contenu téléversé est perdu.

Liens connexes

Mise à jour du micrologiciel de périphérique
Affichage et gestion des mises à jour étagées
Téléchargement du micrologiciel de périphérique

Mise à jour du micrologiciel via l'espace de stockage

Vous pouvez effectuer plusieurs mises à jour de micrologiciel en spécifiant un partage de réseau contenant un espace de stockage valide de progiciels DUP et un catalogue décrivant les progiciels DUP disponibles. Lorsque iDRAC se connecte à l'emplacement du partage réseau et vérifie si des mises à jour sont disponibles, un rapport de comparaison est généré qui répertorie toutes les mises à jour disponibles. Vous pouvez ensuite sélectionner et appliquer les mises à jour requises contenues dans l'espace de stockage du système.

Avant d'effectuer une mise à jour à l'aide de l'espace de stockage, assurez-vous que :

- Un espace de stockage contenant des progiciels de mise à jour (DUP) basés sur Windows et un fichier de catalogue sont créés dans le partage réseau (CIFS ou NFS). Si un fichier de catalogue défini par l'utilisateur n'est pas disponible, **Catalog.xml** est utilisé par défaut.
- Le Lifecycle Controller est activé.
- Vous disposez du privilège de contrôle du serveur pour mettre à jour le micrologiciel pour les périphériques autres que l'iDRAC.

Pour mettre à jour le micrologiciel du périphérique à l'aide d'un espace de stockage :

1. L'interface Web iDRAC7, allez dans **Présentation générale** → **Paramètres iDRAC** → **Mise à jour et restauration** .
   La page **Mise à jour de micrologiciel** s'affiche.
2. Sur l'onglet **Mise à jour**, sélectionnez **Partage réseau** comme **emplacement des fichiers**.
3. Dans la section **Emplacement du catalogue**, entrez les détails de paramétrage du réseau.
   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC7*.
4. Cliquez sur **Vérifier les mises à jour**.
   La section **Détails de la mise à jour** affiche un rapport de comparaison montrant les versions actuelles du micrologiciel et les versions de micrologiciel disponibles dans l'espace de stockage.

   REMARQUE : Toutes les mises à jour de l'espace de stockage qui ne peuvent pas être appliquées au système ou au matériel installé ou non prises en charge ne sont pas incluses dans le rapport de comparaison.
5. Sélectionnez les mises à jour requises et effectuez l'une des opérations suivantes :
   - Pour les images de micrologiciel qui ne nécessitent pas un redémarrage du système hôte, cliquez sur **Installer** (par exemple, le fichier micrologiciel **.d7**).
   - Pour les images de micrologiciel qui nécessitent un redémarrage du système hôte, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**.
   - Pour annuler la mise à jour du micrologiciel, cliquez sur **Annuler**.

   Lorsque vous cliquez sur **Installer Installer et redémarrer** ou **Installer au prochain redémarrage**, le message `Updating Job Queue` (Mise à jour de la file d'attente des tâches) s'affiche.

6. Cliquez sur **File d'attente des tâches** pour afficher la page **File d'attente des tâches**, laquelle vous permet d'afficher et de gérer les mises à jour de micrologiciel étagées ou de cliquer sur **OK** pour actualiser la page et voir l'état de la mise à jour du micrologiciel.

Liens connexes

Mise à jour du micrologiciel de périphérique
Affichage et gestion des mises à jour étagées
Téléchargement du micrologiciel de périphérique
Planification des mises à jour automatiques du micrologiciel

Mise à jour du micrologiciel à l'aide de FTP

Vous pouvez vous connecter directement au site FTP de Dell ou à n'importe quel autre site FTP à partir d'iDRAC pour effectuer les mises à jour des micrologiciels. Vous pouvez utiliser les progiciels de mise à jour basés sur Windows (DUP) et un fichier de catalogue disponibles sur le site FTP au lieu de créer des espaces de stockage personnalisés.

Avant d'effectuer une mise à jour à l'aide de l'espace de stockage, assurez-vous que :

- Le Lifecycle Controller est activé.
- Vous disposez du privilège de contrôle du serveur pour mettre à jour le micrologiciel pour les périphériques autres que l'iDRAC.

Pour mettre à jour le micrologiciel du périphérique à l'aide de FTP :

1. Dans l'interface Web iDRAC7, allez dans **Présentation générale** → **Paramètres iDRAC** → **Mise à jour et restauration** .

   La page **Mise à jour de micrologiciel** s'affiche.
2. Sur l'onglet **Mise à jour** , choisissez **FTP** comme **emplacement des fichiers**.
3. Dans la section **Paramètres du serveur FTP**, entrez les détails FTP.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.
4. Cliquez sur **Check for Update** (Vérifier les mises à jour).
5. Une fois le téléversement terminé, la section **Détails de la mise à jour** affiche un rapport de comparaison montrant les versions actuelles du micrologiciel et les versions de micrologiciel disponibles dans l'espace de stockage.

   REMARQUE : Toutes les mises à jour de l'espace de stockage qui ne sont pas applicables au système ou au matériel installé ou qui ne sont pas prises en charge ne sont pas incluses dans le rapport de comparaison.
6. Sélectionnez les mises à jour requises et effectuez l'une des opérations suivantes :

   – Pour les images de micrologiciel qui ne nécessitent pas un redémarrage du système hôte, cliquez sur **Installer** (par exemple, le fichier micrologiciel **.d7**).
   – Pour les images de micrologiciel qui nécessitent un redémarrage du système hôte, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**.
   – Pour annuler la mise à jour du micrologiciel, cliquez sur **Annuler**.

   Lorsque vous cliquez sur **Installer**, **Installer et redémarrer** ou **Installer au prochain redémarrage**, le message `Updating Job Queue` (Mise à jour de la file d'attente) des tâches s'affiche.
7. Cliquez sur **File d'attente des tâches** pour afficher la page **File d'attente des tâches**, laquelle vous permet d'afficher et de gérer les mises à jour de micrologiciel étagées ou de cliquer sur **OK** pour actualiser la page et voir l'état de la mise à jour du micrologiciel.

Liens connexes

Mise à jour du micrologiciel de périphérique
Affichage et gestion des mises à jour étagées
Téléchargement du micrologiciel de périphérique

Planification des mises à jour automatiques du micrologiciel

Mise à jour du micrologiciel de périphérique à l'aide de RACADM

Pour mettre à jour le micrologiciel des périphériques à l'aide de RACADM, utilisez la sous-commande **update**. Pour en savoir plus, voir le *RACADM Reference Guide for iDRAC7 and CMC* (Guide de référence RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Exemples :

- Pour générer un rapport de comparaison à l'aide d'un espace de stockage de mise à jour :
  ```
  racadm update –f catalog.xml –l //192.168.1.1 –u test –p passwd --
  verifycatalog
  ```
- Pour exécuter toutes les mises à jour applicables à partir d'un espace de stockage de mise à jour en utilisant **myfile.xml** sous la forme d'un fichier de catalogue et effectuer un redémarrage normal :
  ```
  racadm update –f "myfile.xml" –b "graceful" –l //192.168.1.1 –u test –p
  passwd
  ```
- Pour exécuter toutes les mises à jour applicables à partir d'un espace de stockage de mise à jour FTP à l'aide de **Catalog.xml** sous la forme d'un fichier de catalogue :
  ```
  racadm update –f "Catalog.xml" –t FTP –e 192.168.1.20/Repository/Catalog
  ```

Planification des mises à jour automatiques du micrologiciel

Vous pouvez créer une planification périodique selon laquelle l'iDRAC vérifie les nouvelles mises à jour micrologicielles. Au jour et à l'heure planifiés, l'iDRAC se connecte au partage réseau spécifié (CIFS ou NFS) ou au FTP, vérifie les nouvelles mises à jour et applique ou planifie les mises à jour applicables. Un fichier journal sur le serveur distant contient des informations sur l'accès au serveur et les mises à jour de micrologiciel planifiées.

Des mises à jour automatiques sont disponibles uniquement avec la licence iDRAC7 Enterprise.

Vous pouvez planifier les mises à jour automatiques du micrologiciel à l'aide de l'interface Web d'iDRAC ou de RACADM.

REMARQUE : L'adresse IPv6 n'est pas prise en charge pour programmer les mises à jour automatiques du micrologiciel.

Liens connexes

Téléchargement du micrologiciel de périphérique
Mise à jour du micrologiciel de périphérique
Affichage et gestion des mises à jour étagées

Planification de la mise à jour automatique du micrologiciel via l'interface Web

Pour planifier la mise à jour automatique du micrologiciel à l'aide de l'interface Web :

REMARQUE : Ne créez pas la prochaine survenue d'une mise à jour automatique si elle est déjà programmée. Cela remplace la tâche planifiée actuelle.

1. Dans l'interface Web iDRAC7, allez dans **Présentation générale** → **Paramètres iDRAC** → **Mise à jour et restauration** .
   La page **Mise à jour de micrologiciel** s'affiche.
2. Cliquez sur l'onglet **Mise à jour automatique**.
3. Sélectionnez l' option de **sélection de la mise à jour automatique**.

4. Sélectionnez l'une ou l'autre des options suivantes pour indiquer si le redémarrage d'un système est requis après la préparation des mises à jour :
   - **Planifier des mises à jour** : effectuez des mises à jour de micrologiciel sans redémarrer le serveur.
   - **Planifier des mises à jour et redémarrer le serveur** : permet de redémarrer le serveur après la programmation des mises à jour de micrologiciel.
5. Sélectionnez un des éléments suivants pour spécifier l'emplacement des images du micrologiciel :
   - **Réseau** : utilisez le fichier de catalogue depuis un partage réseau (CIFS ou NFS). Saisissez les détails de l'emplacement du partage réseau.
   - **FTP** - Utilisez le fichier de catalogue à partir du site FTP. Saisissez les détails du site FTP.
6. En fonction de la sélection à l'étape 5, entrez les paramètres réseau ou les paramètres FTP.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.
7. Dans la section **Mise à jour de la fenêtre de planification** , spécifiez l'heure de début de la mise à jour de micrologiciel et la fréquence des mises à jour (tous les jours, toutes les semaines ou tous les mois).

   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.
8. Cliquez sur **Planifier la mise à jour**.

   La prochaine tâche planifiée est créée dans la file d'attente des tâches. Cinq minutes après le début de la première instance des tâches récurrentes, la tâche de la prochaine période est créée.

Planification de la mise à jour automatique du micrologiciel à l'aide de RACADM

Pour planifier automatiquement la mise à jour de micrologiciel, utilisez les commandes suivantes :

- Pour activer la mise à jour automatique du micrologiciel :

  ```
  racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
  ```
- Pour afficher l'état de la mise à jour automatique du micrologiciel :

  ```
  racadm get lifecycleController.lcattributes.AutoUpdate
  ```
- Pour planifier l'heure de début et la fréquence de la mise à jour de micrologiciel :

  ```
  racadm AutoUpdateScheduler create -u username –p password –l <location> [-f
  catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt
  <proxytype>] -time < hh:mm> [-dom < 1 – 28,L,’*’> -wom <1-4,L,’*’> -dow <sun-
  sat,’*’>] -rp <1-366> -a <applyserverReboot (1-enabled | 0-disabled)>
  ```

  Par exemple :

  - Pour mettre à jour automatiquement le micrologiciel à l'aide d'un partage CIFS :

    ```
    racadm AutoUpdateScheduler create –u admin –p pwd –l //1.2.3.4/CIFS-share
    –f cat.xml –time 14:30 –wom 1 –dow sun –rp 5 –a 1
    ```
  - Pour mettre à jour automatiquement le micrologiciel à l'aide de FTP :

    ```
    racadm AutoUpdateScheduler create –u admin –p pwd –l ftp.mytest.com –pu
    puser –pp puser –po 8080 –pt http –f cat.xml –time 14:30 –wom 1 –dow sun –
    rp 5 –a 1
    ```
- Pour afficher le calendrier de mise à jour du micrologiciel en cours :

  ```
  racadm AutoUpdateScheduler view
  ```
- Pour désactiver la mise à jour automatique du micrologiciel :

  ```
  racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
  ```
- Pour effacer les détails de planification :

  ```
  racadm AutoUpdateScheduler clear
  ```

Mise à jour du micrologiciel en utilisant l'interface Web CMC

Vous pouvez mettre à jour le micrologiciel d'iDRAC7 des serveurs lames en utilisant l'interface Web CMC.

Pour ce faire :

1. Ouvrez une session dans l'interface Web CMC.
2. Allez sous **Serveur** → **Présentation** → **<nom du serveur>** .

   La page **Condition du du serveur** s'affiche.
3. Cliquez sur **Launch iDRAC Web interface** (Lancer l'interface Web iDRAC) et **iDRAC Firmware Update** (Mise à jour du micrologiciel iDRAC).

Liens connexes

Mise à jour du micrologiciel de périphérique

Téléchargement du micrologiciel de périphérique

Mise à niveau du micrologiciel en utilisant l'interface Web d'iDRAC7

Mise à jour du micrologiciel en utilisant DUP

Avant de mettre à jour le micrologiciel en utilisant DUP (Dell Update Package) :

- Installez et activez les pilotes IPMI et du système géré.
- Activez et démarrez le service WMI (Windows Management Instrumentation) si le système exécute un système d'exploitation Windows.

  REMARQUE : Lors de la mise à jour du micrologiciel iDRAC7 en utilisant l'utilitaire DUP, si des messages d'erreur tels que `usb 5-2: device descriptor read/64, error -71` s'affichent sur la console, ignorez-les.
- Si le système est doté d'hyperviseur ESX, pour que le fichier DUP puisse s'exécuter, arrêtez le service « usbarbitrator » en utilisant la commande `service usbarbitrator stop`

Pour mettre à jour iDRAC7 en utilisant DUP :

1. Téléchargez le fichier DUP en fonction du système d'exploitation installé et exécutez-le sur le système géré.
2. Exécutez le fichier DUP.

   Le micrologiciel est mis à jour. Il n'est pas nécessaire de redémarrer le système à la fin de la mise à jour.

Mise à jour du micrologiel à l'aide de l'interface RACADM

Pour effectuer la mise à jour en utilisant l'interface RACADM :

1. Téléchargez l'image du micrologiciel vers le serveur TFTP ou FTP. Par exemple, **C:\downloads\firmimg.d7**
2. Exécutez la commande RACADM suivante :

   TFTP server:

   - Avec la commande **fwupdate** : `racadm -r <adresse IP iDRAC7> -u <nom_d'utilisateur> -p <mot_de_passe> fwupdate -g -u -a <chemin_d'accès>`

     où *chemin d'accès* est l'emplacement sur le serveur TFTP où **firmimg.d7** est stocké.
   - Avec la commande **update** : `racadm -r <adresse IP iDRAC7> -u <nom_d'utilisateur> -p <mot_de_passe> update –f <nom_de_fichier>`

   FTP server:

   - Avec la commande **fwupdate** : `racadm -r <adresse IP iDRAC7> -u <nom_d'utilisateur> -p <mot_de_passe> fwupdate –f <IP_ftpsrever> <nom_d'utilisateur_ftpserver> <mot_de_passe_ftpserver> –d <chemin_d'accès>`

     où *chemin d'accès* est l'emplacement sur le serveur FTP où **firmimg.d7** est stocké.
   - Avec la commande **update** : `racadm -r <adresse IP iDRAC7> -u <nom_d'utilisateur> -p <mot_de_passe> update –f <nom_de_fichier>`

   Pour plus d'informations, voir la commande **fwupdate** dans le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Mise à jour du micrologiciel en utilisant le services à distance Lifecycle Controller

Pour en savoir plus sur la mise à jour du micrologiciel à l'aide des services à distances Lifecycle Controller, voir le *Lifecycle Controller Remote Services Quick Start Guide* (Guide de démarrage rapide des services à distance Lifecycle Controller) disponible à l'adresse **dell.com/support/manuals**.

Affichage et gestion des mises à jour étagées

Vous pouvez afficher et supprimer les tâches planifiées, notamment les tâches de configuration et de mise à jour. Il s'agit d'une fonctionnalité sous licence. Toutes les tâches en attente de s'exécuter au prochain démarrage peuvent être supprimées.

Liens connexes

Mise à jour du micrologiciel de périphérique

Affichage et gestion des mises à jour étagées à l'aide de l'interface Web iDRAC7

Pour afficher une liste des tâches planifiées à l'aide de l'interface Web iDRAC, allez sous **Présentation → Serveur → File d'attente des tâches**. La page **File d'attente des tâches** affiche l'état des tâches de la file d'attente du Lifecycle Controller. Pour en savoir plus sur les champs affichés, voir l'*aide en ligne iDRAC7*.

Pour supprimer des tâches, sélectionnez les tâches à supprimer et cliquez sur **Supprimer**. La page est actualisée et les tâches sélectionnées sont supprimées de la file d'attente du Lifecycle Controller. Vous pouvez supprimer toutes les tâches de la file d'attente censées s'exécuter au prochain démarrage. Vous ne pouvez cependant pas supprimer des tâches actives, c'est-à-dire des tâches dont l'état est *En cours d'exécution* ou *En cours de téléchargement*.

Vous devez disposer des privilèges de contrôle du serveur pour supprimer des tâches.

Affichage et gestion des mises à jour étagées à l'aide de RACADM

Pour afficher les mises à jour étagées à l'aide de RACADM, utilisez la sous-commande **jobqueue**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Restauration du micrologiciel du périphérique

Vous pouvez restaurer le micrologiciel d'iDRAC ou d'un périphérique pris en charge par Lifecycle Controller. Effectuez la restauration du micrologiciel pour plusieurs périphériques en un seul démarrage du système.

Restaurez le micrologiciel même lorsque la mise à jour a été précédemment effectuée à l'aide d'une autre interface. Par exemple, si le micrologiciel a été mis à jour à l'aide de l'interface GUI de Lifecycle Controller, vous pouvez restaurer le micrologiciel à l'aide de l'interface Web d'iDRAC7.

Vous pouvez effectuer la mise à jour du micrologiciel sur les composants suivants :

- iDRAC
- BIOS
- Carte d'interface réseau (NIC)
- Unité d'alimentation (PSU)
- Contrôleur RAID

REMARQUE : Il est impossible d'effectuer une restauration de micrologiciel pour le Lifecycle Controller, les Diagnostics, les packs de pilotes et CPLD.

Avant de restaurer le micrologiciel, assurez-vous que :

- Vous disposez des droits de configuration nécessaires pour restaurer le micrologiciel d'iDRAC.
- Vous disposez des droits de contrôle du serveur et avez activé Lifecycle Controller pour restaurer le micrologiciel d'un périphérique autre que l'iDRAC.

Vous pouvez restaurer la version précédente du micrologiciel en utilisant les méthodes suivantes :

- Interface Web iDRAC7
- Interface Web CMC
- CLI RACADM (iDRAC7 et CMC)
- Lifecycle Controller
- les services à distance Liffecycle Controller.

Liens connexes

Restauration du micrologiciel à l'aide de l'interface Web d'iDRAC7
Restauration du micrologiciel en utilisant l'interface Web CMC
Restauration du micrologiciel en utilisant l'interface RACADM
Restauration du micrologiciel en utilisant Lifecycle Controller
Restauration micrologiciel en utilisant les services distants Lifecycle Controller

Restauration du micrologiciel à l'aide de l'interface Web d'iDRAC7

Pour restaurer un micrologiciel de périphérique :

1. L'interface Web iDRAC7, allez dans **Présentation** → **Paramètres iDRAC** → **Mise à jour et restauration** → **Restauration** .

   Tous les périphériques pour lesquels vous pouvez restaurer le micrologiciel s'affichent dans la page de **Restauration**. Vous pouvez afficher le nom du périphérique, les périphériques associés, la version du micrologiciel actuellement installé, ainsi que la version de restauration du micrologiciel disponible.
2. Sélectionnez un ou plusieurs périphériques pour lesquels vous voulez restaurer le micrologiciel.
3. Selon les périphériques sélectionnés, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**. Si seul l'iDRAC est sélectionné, cliquez sur **Installer**.

   Lorsque vous cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**, le message « Mise à jour de la file d'attente des tâches » s'affiche.
4. Cliquez sur **la file d'attente des tâches**.

   La page **File d'attente des tâches** s'affiche, où vous pouvez afficher et gérer les mises à jour du micrologiciel par étapes.

   REMARQUE :

   - Lorsque la restauration est en cours, le processus de restauration continue de s'exécuter en arrière-plan, même si vous quittez la page.
   - Si vous restaurez les valeurs de configuration par défaut d'iDRAC7, l'adresse IP iDRAC7 192.168.0.120 est restaurée. Vous pouvez accéder à iDRAC7 en utilisant cette adresse IP ou redéfinir l'adresse d'iDRAC7 en utilisant l'interface locale RACADM ou en appuyant sur F2 (l'interface distance RACADM nécessite un accès réseau).

   Un message d'erreur s'affiche si :

   - Vous ne disposez pas des droits de contrôle du serveur pour restaurer des micrologiciels autres que l' iDRAC ou des privilèges de configuration pour restaurer le micrologiciel d'iDRAC.
   - La restauration de micrologiciel est déjà en cours dans une autre session.
   - Les mises à jour sont prêtes à s'exécuter ou sont déjà en cours.

   Le Lifecycle Controller est désactivé ou dans un état de restauration et vous tentez d'effectuer une restauration du micrologiciel d'un périphérique autre que l'iDRAC. Un message d'avertissement approprié s'affiche, ainsi que les étapes permettant d'activer Lifecycle Controller.

Restauration du micrologiciel en utilisant l'interface Web CMC

Pour effectuer la restauration en utilisant l'interface Web CMC :

1. Ouvrez une session dans l'interface Web CMC.
2. Accédez à **Présentation du serveur** → **<nom du serveur>**.

   La page **Condition du serveur** s'affiche.
3. Cliquez sur **Lancer l'iDRAC** et effectuez la restauration du micrologiciel du périphérique telle que mentionnée dans la section Restauration du micrologiciel à l'aide de l'interface Web de l'iDRAC7 .

Restauration du micrologiciel en utilisant l'interface RACADM

Pour la restauration du micrologiciel du périphérique à l'aide de racadm :

1. Vérifiez l'état de la restauration et le FQDD à l'aide de la commande `swinventory` :
   `racadm swinventory`

   La `version de restauration` du périphérique pour lequel vous voulez restaurer le micrologiciel doit être `disponible`. De plus, notez le FQDD.

2. Restauration du micrologiciel du périphérique à l'aide de :
   `racadm rollback <FQDD>`

   Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACDAM pour iDRAC7 et CMC* disponible à l'adresse **dell.com/support/manuals**.

Restauration du micrologiciel en utilisant Lifecycle Controller

Pour plus d'informations, voir le *Lifecycle Controller User's Guide* (Guide d'utilisation de Lifecycle Controller) disponible à l'adresse **dell.com/support/manuals**.

Restauration micrologiciel en utilisant les services distants Lifecycle Controller

Pour en savoir plus, voir le *Lifecycle Controller Remote Services Quick Start Guide* (Guide de démarrage rapide des services distants du Lifecycle Controller) disponible à l'adresse **dell.com/support/manuals**.

Restauration d'iDRAC7

iDRAC7 prend en charge deux images de système d'exploitation pour disposer d'un iDRAC7 amorçable. Dans le cas d'un problème catastrophique imprévu où les deux chemins d'amorçage sont perdus :

- Le chargeur de démarrage iDRAC7 détecte qu'il n'existe aucune image amorçable.
- Le voyant d'intégrité et d'identification du système clignote à une fréquence de ~1/2 seconde. (Le voyant se trouve à l'arrière sur un serveur en rack ou de type tour et à l'avant sur un serveur lame.)
- Le chargeur de démarrage appelle le logement de la carte SD.
- Formatez une carte SD avec FAT s'il s'agit d'un système d'exploitation Windows ou avec EXT3 s'il s'agit d'un système d'exploitation LInux.
- Copiez **firmimg.d7** vers la carte SD.
- Insérez la carte SD dans le serveur.
- Le chargeur de démarrage détecte la carte SD, active le voyant fixe orange, lit firmimg.d7, reprogramme iDRAC7 et démarre iDRAC7.

Utilisation du serveur TFTP

Vous pouvez utiliser le serveur TFTP (Trivial File Transfer Protocol) pour mettre à niveau vers une version supérieure ou antérieure le micrologiciel iDRAC7 ou installer des certificats.Il est utilisé dans les interfaces de ligne de commande SM-CLP et RACADM pour transférer des fichiers vers et depuis iDRAC7. Le serveur TFTP doit être accessible en utilisant l'adresse IP iDRAC7 ou le nom DNS.

REMARQUE : Si vous utilisez l'interface Web iDRAC7 pour transférer des certificats et mettre à jour le micrologiciel, TFTP n'est pas nécessaire.

Vous pouvez utilisez la commande `netstat -a` dans les systèmes d'exploitation Windows ou Linux pour déterminer si un serveur TFTP est actif. Le port par défaut pour TFTP est 69. Si le serveur TFTP n'est actif, procédez comme suit :

- Recherchez un autre ordinateur sur le réseau exécutant un service TFTP.
- Installez un serveur TFTP sur le système d'exploitation.

Sauvegarde du profil du serveur

Vous pouvez sauvegarder la configuration du système, y compris les images du micrologiciel installé sur divers composants, tels que le BIOS, RAID, NIC, iDRAC, Lifecycle Controller et les cartes fille réseau (NDC) et les paramètres de configuration de ces composants. L'opération de sauvegarde inclut également les données de configuration de disque dur, la carte mère et les pièces remplacées. La sauvegarde crée un fichier unique, que vous pouvez enregistrer sur une carte SD vFlash ou le partage réseau (CIFS ou NFS).

Vous pouvez également activer et planifier des sauvegardes périodiques du micrologiciel, ainsi que la configuration du serveur en fonction d'un jour, une semaine ou un mois particulier.

La fonction de sauvegarde est sous licence et disponible avec la licence iDRAC7 Enterprise.

Avant d'effectuer une opération de sauvegarde, assurez-vous que :

- L'option CSIOR (Collect System Inventory On Reboot) est activée. Si la fonction CSIOR est désactivée et si vous lancez une opération de sauvegarde, le message suivant s'affiche :
  `System Inventory with iDRAC may be stale,start CSIOR for updated inventory`
- Pour effectuer la sauvegarde sur une carte SD vFlash :
  - une carte SD vFlash prise en charge Dell est insérée, activée et initialisée.
  - la carte SD vFlash dispose d'un espace suffisant pour stocker le fichier de sauvegarde.

Le fichier de sauvegarde contient des données utilisateur sensibles chiffrées, des informations de configuration et des images micrologicielles que vous pouvez utiliser pour l'opération de restauration.

Les événements de sauvegarde et de restauration sont enregistrés dans le journal Lifecycle.

Liens connexes

Planification de la sauvegarde automatique du profil de serveur
Importation du profil du serveur

Sauvegarde du profil du serveur à l'aide de l'interface Web iDRAC7

Pour sauvegarder le profil du serveur à l'aide de l'interface Web iDRAC7 :

1. Accédez à **Présentation générale** → **Paramètres iDRAC** → **Profil du serveur** .
   La page **Sauvegarde et restauration du profil du serveur** s'affiche.
2. Sélectionnez un des éléments suivants pour enregistrer l'image du fichier de sauvegarde :
   - **réseau** pour enregistrer l'image du fichier de sauvegarde sur un partage CIFS ou NFS.
   - **vFlash** pour enregistrer l'image du fichier de sauvegarde sur la carte vFlash.
3. Saisissez le nom du fichier de sauvegarde et la phrase de passe de chiffrement (facultatif).
4. Si **Réseau** est sélectionné comme emplacement du fichier, saisissez les paramètres de réseau.
   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.
5. Cliquez sur **Sauvegarder maintenant**.
   L'opération de sauvegarde est initialisée et vous pouvez afficher l'état sur la page **File d'attente des tâches**. Après une opération réussie, le fichier de sauvegarde est créée dans l'emplacement spécifié.

Sauvegarde du profil du serveur à l'aide de RACADM

Pour sauvegarder le profil du serveur à l'aide de RACADM, utilisez la sous-commande **systemconfig backup**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Planification de la sauvegarde automatique du profil de serveur

Vous pouvez activer et planifier des sauvegardes périodiques du micrologiciel, ainsi que de la configuration du serveur en fonction d'un jour, d'une semaine ou d'un mois particulier.

Avant de planifier une sauvegarde automatique de profil de serveur, assurez-vous que :

- Les options Lifecycle Controller et CSIOR (Collect System Inventory On Reboot) sont activées.
- Network Time Protocol (NTP) est activé de manière à ce que la dérive en temps réel n'ait pas d'incidence sur la durée d'exécution des tâches planifiées et sur l'heure de création de la prochaine tâche planifiée.
- Pour effectuer la sauvegarde sur une carte SD vFlash :
  - une carte SD vFlash prise en charge Dell est insérée, activée et initialisée.
  - la carte SD vFlash dispose d'un espace suffisant pour stocker le fichier de sauvegarde.

REMARQUE : L'adresse IPv6 n'est pas prise en charge pour la planification de la sauvegarde automatique du profil de serveur.

Planification de la sauvegarde automatique du profil de serveur via l'interface Web

Pour planifier la sauvegarde automatique du profil de serveur :

1. Dans l'interface Web de l'iDRAC7, allez à **Présentation générale → Paramètres iDRAC → Profil du serveur**.
   La page **Sauvegarde et exportation du profil du serveur** s'affiche.
2. Cliquez sur l'onglet de **sauvegarde automatique** .
3. Sélectionnez l'option **Activer la sauvegarde automatique** .
4. Sélectionnez un des éléments suivants pour enregistrer l'image du fichier de sauvegarde :
   - **Réseau** pour enregistrer l'image du fichier de sauvegarde sur un partage CIFS ou NFS.
   - **vFlash** pour enregistrer le fichier image de sauvegarde sur la carte vFlash.
5. Saisissez le nom du fichier de sauvegarde et la phrase de passe de chiffrement (facultatif).
6. Si **Réseau** est bien sélectionné comme emplacement de fichier, entrez les paramètres du réseau. Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC7*.
7. Dans la section **Calendrier de la fenêtre de sauvegarde**, spécifiez l'heure de début de l'opération de sauvegarde et la fréquence de l'opération (tous les jours, toutes les semaines ou tous les mois).
   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.
8. Cliquez sur **Planifier la sauvegarde**.
   Une tâche récurrente est représentée dans la file d'attente des tâches avec une date et une heure de début pour la prochaine sauvegarde programmée. Cinq minutes après le démarrage de la première instance de la tâche, la tâche de la période de temps suivante est créée. La sauvegarde du profil du serveur est effectuée à la date et à l'heure spécifiées.

Planification de sauvegarde du profil de serveur à l'aide de RACADM

Pour activer la sauvegarde automatique, utilisez la commande suivante :

```
racadm set lifecyclecontroller.lcattributes.autobackup Enabled
```

Pour planifier une opération de sauvegarde de profil de serveur :

```
racadm systemconfig backup –f <filename> <target> [-n <passphrase>] -time
<hh:mm> -dom <1-28,L,’*’> -dow<*,Sun-Sat> -wom <1-4, L,’*’> -rp <1-366>-mb <Max
Backups>
```

Pour afficher le calendrier de sauvegarde actuel :

```
racadm systemconfig getbackupscheduler
```

Pour désactiver la sauvegarde automatique, utilisez la commande suivante :

```
racadm set lifecyclecontroller.lcattributes.autobackup Dis\abled
```

Pour effacer le calendrier de sauvegarde :

```
racadm systemconfig clearbackupscheduler
```

Pour plus d'informations, voir le manuel RACADM Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

Importation du profil du serveur

Vous pouvez utiliser le fichier image de sauvegarde pour restaurer la configuration et le micrologiciel sur le même serveur ou un autre serveur ayant la même configuration, sans avoir à redémarrer le serveur.

La fonction d'importation s'utilise sans licence.

REMARQUE : Afin que l'opération de restauration réussisse, le numéro de service du système et le numéro de service du fichier de sauvegarde doivent être identiques. L'opération de restauration s'applique à tous les composants système identiques présents dans le même emplacement (par exemple, dans le même logement) - tel que capturé dans le fichier de sauvegarde. Si les composants sont différents ou ne se trouvent pas dans le même emplacement, ils ne sont pas modifiés et les échecs de restauration sont journalisés dans le journal Lifecycle.

Avant d'effectuer une opération d'importation, assurez-vous que le Lifecycle Controller est activé. S'il ne l'est pas et que vous initialisez une opération d'importation, le message suivant s'affiche :

```
Lifecycle Controller is not enabled, cannot create Configuration job.
```

Lorsque l'importation est déjà en cours et que vous lancez de nouveau une opération d'importation, un message d'erreur s'affiche :

```
Restore is already running
```

Les événements d'importation sont enregistrés dans le journal Lifecycle.

Liens connexes

Séquence desopérations de restauration

Importation du profil du serveur à l'aide de l'interface Web iDRAC7

Pour importer le profil du serveur à l'aide de l'interface Web iDRAC7 :

1. Accédez à **Présentation générale** → **Paramètres iDRAC** → **Profil de serveur** → **Importer**.
   La section **Importer le profil de serveur** s'affiche.
2. Sélectionnez un des éléments suivants pour spécifier l'emplacement du fichier de sauvegarde :
   - **Réseau**
   - **vFlash**
3. Saisissez le nom du fichier de sauvegarde et la phrase de passe de déchiffrement (facultatif).
4. Si **Réseau** est sélectionné comme emplacement du fichier, saisissez les paramètres de réseau.
   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.

5. Sélectionnez l'une des options suivantes pour la **configuration des disques virtuels et des données du disque dur** :
   - **Conserver** : conserve les informations sur le niveau de RAID, le disque virtuel, les attributs de contrôleur et le disque dur dans le système et restaure l'état du système à un état antérieur à l'aide du fichier image de sauvegarde.
   - **Supprimer et remplacer** : supprime et remplace les informations sur le niveau de RAID, le disque virtuel, les attributs de contrôleur et la configuration du disque dur dans le système à l'aide des données du fichier image de sauvegarde.
6. Cliquez sur **Importer**.

   L'importation de profil de serveur est lancée.

Importation du profil du serveur à l'aide de RACADM

Pour importer le profil du serveur à l'aide de RACADM, utilisez la commande **systemconfig restore**. Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC* disponible à l'adresse **dell.com/support/manuals**.

Séquence desopérations de restauration

La séquence des opérations de restauration est la suivante :

1. Le système hôte s'éteint.
2. Les informations des fichiers de sauvegarde sont utilisées pour restaurer le Lifecycle Controller.
3. Le système hôte s'allume.
4. Le processus de restauration du micrologiciel et de la configuration pour les périphériques est terminé.
5. Le système hôte s'éteint.
6. Le processus de restauration du micrologiciel iDRAC et de la configuration est terminé.
7. iDRAC redémarre.
8. Le système hôte restauré s'allume pour fonctionner à nouveau normalement.

Surveillance d'iDRAC7 à l'aide d'autres outils de gestion de systèmes

Vous pouvez détecter et surveiller iDRAC7 en utilisant Dell Management Console et Dell OpenManage Essentials. Vous pouvez également utiliser Dell Remote Access Configuration Tool (DRACT) pour détecter les iDRAC, mettre à jour le micrologiciel et configurer Active Directory. Pour plus d'informations, voir les guides d'utilisation correspondants.

4

Configuration d'iDRAC7

iDRAC7 permet de configurer les propriétés iDRAC7 et de définir des utilisateurs et des alertes pour exécuter les tâches de gestion à distance.

Avant de configurer iDRAC7, veillez à configurer les paramètres réseau iDRAC7 et le navigateur pris en charge et à mettre à jour les licences nécessaires. Pour plus d'informations sur les fonctions utilisables sous licence dans iDRAC7, voir Gestion des licences.

Vous configurez iDRAC7 en utilisant :

- Interface Web iDRAC7
- RACADM
- les services à distance (voir le *Guide d'utilisation des services à distance Lifecycle Controller*) ;
- IPMITool (voir le *Guide d'utilisation de Baseboard Management Controller Management*).

Pour configurer iDRAC7 :

1. Ouvrez une session dans iDRAC7.
2. Modifiez les paramètres réseau, si nécessaire.

   REMARQUE : Si vous avez défini les paramètres réseau iDRAC7 en utilisant l'utilitaire de configuration d'iDRAC pendant la définition de l'adresse IP iDRAC7 IP, ignorez cette étape.
3. Définissez les interfaces d'accès à iDRAC7.
4. Configurez l'écran du panneau avant.
5. Définissez l'emplacement du système.
6. Configurez le fuseau horaire et le protocole NTP (Network Time Protocol - Protocole de temps de réseau), le cas échéant.
7. Définissez les modes de communication secondaires suivants avec iDRAC7 :
   - IPMI ou RAC série
   - IPMI sériel sur LAN
   - IPMI sur le LAN
   - Client SSH ou Telnet
8. Obtenez les certificats nécessaires.
9. Ajoutez et configurez des utilisateurs iDRAC7 avec des privilèges.
10. Configurez et activez les alertes par e-mail, les interruptions SNMP ou les alertes IPMI.
11. Définissez la politique de limitation d'alimentation, si nécessaire.
12. Affichez le dernier écran de blocage.
13. Configurez la console virtuelle et média virtuel, si nécessaire.
14. Configurez la carte vFlash, si nécessaire.
15. Définissez le premier périphériques de démarrage, si nécessaire.
16. Définissez la connexion directe entre le SE et iDRAC, le cas échéant.

Liens connexes

Affichage des informations iDRAC7

Vous pouvez afficher les propriétés de base d'iDRAC7.

Affichage des informations iDRAC7 à l'aide de l'interface Web

Dans l'interface d'iDRAC7, accédez à **Présentation générale** → **Paramètres iDRAC** → **Propriétés** pour afficher les informations suivantes associées à iDRAC7. Pour plus d'informations sur les propriétés, voir l'*Aide en ligne d'iDRAC7*.

- Type de périphérique
- Version matérielle et du micrologiciel
- Dernière mise à jour du micrologiciel
- Heure RAC
- Nombre de sessions actives possibles
- Nombre de sessions actives en cours
- Le LAN est activé ou désactivé
- Version d'IPMI
- Informations de barre de titre de l'interface utilisateur
- Paramètres réseau
- Paramètres IPv4
- Paramètres IPv6

Affichage des informations iDRAC7 en utilisant l'interface RACADM

Pour afficher les informations iDRAC7 en utilisant l'interface RACADM, consultez les informations relatives à la sous-commande `getsysinfo` ou `get` dans le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande de l'interface RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Modification des paramètres réseau

Après avoir configuré les paramètres réseau iDRAC7 en utilisant l'utilitaire de configuration d'iDRAC, vous pouvez également modifier les paramètres en utilisant l'iinterface Web d'iDRAC7, l'interface RACADM, Lifecycle Controller, Dell Deployment Toolkit et Server Administrator (après avoir démarré dans le système d'exploitation). Pour plus d'informations sur les outils et les paramètres de privilèges, voir les guides d'utilisation correspondants.

Pour pouvoir modifier les paramètres réseau en utilisant l'interface Web d'iDRAC7 ou RACADM, vous devez disposer des privilèges de **Configuration**.

REMARQUE : La modification des paramètres réseau peut mettre fin aux connexions réseau en cours à iDRAC7.

Modification des paramètres réseau en utilisant l'interface Web

Pour modifier les paramètres réseau iDRAC7 :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau**.
   La page **Réseau** s'affiche.
2. Spécifiez les paramètres réseau, paramètres communs, IPv4, IPv6, IPMI et/ou paramètres VLAN, selon vos besoins, puis cliquez sur **Appliquer**.
   Si vous sélectionnez **Carte réseau auto-dédiée** sous **Paramètres réseau**, lorsque la sélection des cartes réseau de l'iDRAC est un LOM partagé (1, 2, 3, ou 4) et qu'une liaison est détectée sur la carte réseau dédiée de l'iDRAC, l'iDRAC modifie sa sélection de cartes réseau pour utiliser la carte réseau dédiée. Si aucune liaison n'est détectée sur la carte réseau dédiée, l'iDRAC utilise alors le LOM partagé. Le temps d'arrêt du passage de partagé à dédié est de 5 secondes et le temps d'arrêt de dédié à partagé est de 30 secondes. Vous pouvez configurer le temps d'arrêt à l'aide de RACADM ou WS-MAN.
   Pour plus d'informations sur les champs, voir l'*aide en ligne d'iDRAC7*.

Modification des paramètres réseau à l'aide de l'interface locale RACADM

Pour générer la liste des propriétés réseau disponibles, tapez la commande suivante :

REMARQUE : Vous pouvez utiliser les commandes **getconfig** et **config** ou les commandes **get** et **set** avec les objets RACADM.

- Avec la commande **getconfig** : `racadm getconfig -g cfgLanNetworking`
- Avec la commande **get** : `racadm get iDRAC.Nic`

Pour utiliser DHCP pour obtenir une adresse IP, utilisez la commande suivante pour écrire l'objet **cfgNicUseDhcp** ou **DHCPEnable** et activer cette fonctionnalité :

- Avec la commande **config** : `racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1`
- Avec la commande **set** : `racadm set iDRAC.IPv4.DHCPEnable 1`

L'exemple suivant montre comment la commande peut être utilisée pour configurer les propriétés réseau LAN souhaitées :

- Utilisation de la commande **config** :

```
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
```

- Avec la commande **set** :

```
racadm set iDRAC.Nic.Enable 1 racadm set iDRAC.IPv4.Address 192.168.0.120
racadm set iDRAC.IPv4.Netmask 255.255.255.0 racadm set iDRAC.IPv4.Gateway
192.168.0.120 racadm set iDRAC.IPv4.DHCPEnable 0 racadm set
iDRAC.IPv4.DNSFromDHCP 0 racadm set iDRAC.IPv4.DNS1 192.168.0.5 racadm set
iDRAC.IPv4.DNS2 192.168.0.6 racadm set iDRAC.Nic.DNSRegister 1 racadm set
iDRAC.Nic.DNSRacName RAC-EK00002 racadm set iDRAC.Nic.DNSDomainFromDHCP 0
racadm set iDRAC.Nic.DNSDomainName MYDOMAIN
```

REMARQUE : Si la commande **cfgNicEnable** ou **iDRAC.Nic.Enable** est définie sur **0**, le LAN iDRAC7 est désactivé, même si DHCP est activé.

Configuration du filtrage IP et du blocage IP

En complément de l'authentification des utilisateurs, utilisez les options suivantes pour renforcer la sécurité de l'accès à iDRAC7 :

- Le filtrage IP limite la plage d'adresses IP des clients qui accèdent à iDRAC7. Il compare l'adresse IP de la connexion entrante à la plage définie et permet l'accès à iDRAC7 uniquement depuis une station de gestion dont l'adresse IP se trouve dans la plage. Toutes les autres demandes de connexion sont rejetées.
- Le blocage IP détermine de manière dynamique un nombre excessif d'échecs de connexion depuis une adresse IP donnée et empêche (bloque) l'adresse de se connecter à iDRAC7 pendant une période prédéfinie. Le blocage inclut :
  - le nombre d'échecs de connexion autorisé ;
  - le délai en secondes au cours duquel ces échecs doivent se produire ;
  - le délai en secondes pendant lequel l'adresse IP bloquée ne peut pas établir de session lorsque le nombre d'échecs autorisés est atteint.

Les échecs de connexion d'une adresse IP sont enregistrés par un compteur interne. Lorsque l'utilisateur parvient à se connecter, l'historique des échecs est effacé et le compteur est réinitialisé.

REMARQUE : Lorsque des tentatives de connexion sont refusées depuis l'adresse IP du client, certains clients SSH peuvent afficher le message suivant : `identification d'échange ssh : connexion fermée par l'hôte distant`.

REMARQUE : Si vous utilisez DTK (Dell Deployment Toolkit), voir le *Guide d'utilisation Dell Deployment Toolkit* pour plus d'informations sur les privilèges.

Configurer le filtrage IP et le blocage IP en utilisant l'interface Web iDRAC7

Vous devez avoir défini le privilège de configuration iDRAC7 pour pouvoir exécuter ces étapes.

Pour configurer le filtrage IP et le blocage IP :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → Réseau**.
   La page **Réseau** s'affiche.
2. Cliquez sur **Paramètres avancés**.
   L'écran **Sécurité du réseau** s'affiche.
3. Définissez les paramètres de filtrage IP et de blocage IP.
   Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC7*.

4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration du filtrage IP et du blocage IP en utilisant l'interface RACADM

Vous devez disposer du privilège de configuration iDRAC7 pour pouvoir exécuter ces opérations.

Pour configurer le filtrage IP et le blocage IP, utilisez les objets RACADM suivants :

- Avec la commande **config** :
  - cfgRacTuneIpRangeEnable
  - cfgRacTuneIpRangeAddr
  - cfgRacTuneIpRangeMask
  - cfgRacTuneIpBlkEnable
  - cfgRacTuneIpBlkFailCount
  - cfgRacTuneIpBlkFailWindow
- Avec la commande **set**, utilisez les objets du groupe **iDRAC.IPBlocking** :
  - RangeEnable
  - RangeAddr
  - RangeMask
  - BlockEnable
  - FailCount
  - FailWindow
  - PenaltyTime

La propriété **cfgRacTuneIpRangeMask** ou **RangeMask** est appliquée à l'adresse IP entrante et à la propriété **cfgRacTuneIpRangeAddr** ou **RangeAddr**. Si les résultats sont identiques, la demande de connexion entrante est autorisée à accéder à iDRAC7. Une connexion depuis des adresses IP en dehors de cette plage génère une erreur.

La connexion a lieu si l'expression suivante est égale à zéro :

- Utilisation de la syntaxe héritée : `cfgRacTuneIpRangeMask & (<adresse_IP_entrante> ^ cfgRacTuneIpRangeAddr)`
- Utilisation de la nouvelle syntaxe : `RangeMask & (<adresse_IP_entrante> ^ RangeAddr)`

où & est l'opérateur de bits AND des quantités et ^ est l'opérateur de bits OR exclusif.

Exemples pour le filtrage IP

- Les commandes RACADM suivantes bloquent toutes les adresses IP, sauf l'adresse 192.168.0.57 :
  - Utilisation de la commande **config** :

    ```
    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
    ```

  - Utilisation de la commande **set** :

    ```
    racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57 racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
    ```

- Pour restreindre les connexions à un petit ensemble de quatre adresses IP contiguës (par exemple, 192.168.0.212 à 192.168.0.215), sélectionnez tout, sauf les deux bits les plus bas dans le masque :
  - Utilisation de la commande **set** :

    ```
    racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212 racadm set iDRAC.IPBlocking.RangeMask 255.255.255.252
    ```

Le dernier octet du masque de plage est défini sur 252, l'équivalent décimal de 11111100b.

Exemples pour le blocage IP

- L'exemple suivant empêche une adresse IP de station de gestion d'établir une session pendant cinq minutes si l'adresse a subi cinq échecs de tentative de connexion pendant une minute.
  - Utilisation de la commande **config** :

    ```
    racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1 racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5 racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
    ```
  - Utilisation de la commande **set** :

    ```
    racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set iDRAC.IPBlocking.FailCount 5 racadm set iDRAC.IPBlocking.FailWindow 60
    ```
- L'exemple suivant empêche plus de trois échecs de tentatives par minute et toute tentative de connexion supplémentaire par heure.
  - Utilisation de la commande **config** :

    ```
    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
    ```
  - Utilisation de la commande **set** :

    ```
    racadm set iDRAC.IPBlocking.BlockEnable 1 racadm set iDRAC.IPBlocking.FailCount 3 racadm set iDRAC.IPBlocking.FailWindow 60 racadm set iDRAC.IPBlocking.PenaltyTime 3600
    ```

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration des services

Vous pouvez configurer et activer les services suivants sur iDRAC7 :

- Configuration locale — Désactiver l'accès à la configuration iDRAC7 (depuis le système hôte) en utilisant l'interface locale RACADM et l'utilitaire de configuration iDRAC .
- Serveur Web — Activer l'accès à l'interface Web iDRAC7. Si vous désactivez l'option, utilisez l'interface locale RACADM pour réactiver le Serveur Web, puisque la désactivation du Serveur Web désactive aussi l'interface distante RACADM.
- SSH — Accès à iDRAC7 via le micrologiciel de RACADM.
- Telnet — Accès à iDRAC7 via le micrologiciel de RACADM.
- Interface distante RACADM — Accès à distance à iDRAC7.
- Agent SNMP — Active la prise en charge des requêtes SNMP (opérations GET, GETNEXT et GETBULK) dans iDRAC7.
- Agent de récupération de système automatique — Activer le dernier écran de blocage système.
- Serveur VNC - Activer le serveur VNC avec ou sans le cryptage SSL.

Configuration des services en utilisant l'interface Web

Pour configurer les services en utilisant l'interface Web iDRAC7 :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → Services**.
   La page **Services** s'affiche.
2. Entrez les informations requises, puis cliquez sur **Appliquer**.
   Pour plus d'informations sur les paramètes, voir l'*aide en ligne d'iDRAC7*.

Configuration des services à l'aide de l'interface RACADM

Pour activer et configurer les différents services à l'aide de RACADM :

- Utilisez les objets suivants avec la commande **config** :
  - cfgRacTuneLocalConfigDisable
  - cfgRacTuneCtrlEConfigDisable
  - cfgSerialSshEnable
  - cfgRacTuneSshPort
  - cfgSsnMgtSshIdleTimeout
  - cfgSerialTelnetEnable
  - cfgRacTuneTelnetPort
  - cfgSsnMgtTelnetIdleTimeout
  - cfgRacTuneWebserverEnable
  - cfgSsnMgtWebserverTimeout
  - cfgRacTuneHttpPort
  - cfgRacTuneHttpsPort
  - cfgRacTuneRemoteRacadmEnable
  - cfgSsnMgtRacadmTimeout
  - cfgOobSnmpAgentEnable
  - cfgOobSnmpAgentCommunity
- Utilisez les objets dans les groupes de l'objet suivants à l'aide de la commande **set** :
  - iDRAC.LocalSecurity
  - iDRAC.LocalSecurity
  - iDRAC.SSH
  - iDRAC.Webserver
  - iDRAC.Telnet
  - iDRAC.Racadm
  - iDRAC.SNMP

Pour plus d'informations sur ces objets, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC), disponible à l'adresse **dell.com/support/manuals**.

Activation ou désactivation de la redirection HTTPs

Si vous ne souhaitez pas de redirection automatique de HTTP à HTTPs en raison d'un avertissement concernant le certificat iDRAC par défaut ou en tant que paramètre temporaire de débogage, vous pouvez configurer l'iDRAC de sorte

que la redirection de port http (la valeur par défaut est 80) vers le port https (la valeur par défaut est 443) est désactivée. Par défaut, elle est activée et vous devez vous déconnecter, puis vous reconnecter à l'iDRAC pour que ce paramètre prenne effet. Lorsque vous désactivez cette fonction, un message d'avertissement s'affiche.

Vous devez disposer du privilège de configuration iDRAC pour activer ou désactiver la redirection HTTPs.

Un événement est enregistré dans le fichier journal du Lifecycle Controller lorsque cette fonction est activée ou désactivée.

Pour désactiver le protocole HTTP à HTTPs pour la redirection :

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

Pour activer le protocole HTTP à HTTPs pour la redirection :

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

Pour afficher l'état de la redirection HTTP à HTTPs :

```
racadm get iDRAC.Webserver.HttpsRedirection
```

Utilisation du client VNC pour gérer le serveur distant

Vous pouvez utiliser un client VNC standard ouvert pour gérer le serveur distant en utilisant les ordinateurs de bureau et des périphériques mobiles tels que Dell Wyse PocketCloud. Lorsque des serveurs d'un centre de données cessent de fonctionner, l'iDRAC ou le système d'exploitation envoie une alerte sur la console de la station de gestion. La console envoie un e-mail ou un SMS sur un appareil mobile avec les informations requises et lance l'application de visualisation VNC sur la station de gestion. Ce visualiseur VNC peut se connecter au système d'exploitation/à l'hyperviseur du serveur et fournir l'accès au clavier, à l'écran et à la souris du serveur hôte pour effectuer les corrections nécessaires. Avant de lancer le client VNC, vous devez activer le serveur VNC et configurer les paramètres du serveur VNC dans l'iDRAC, tels que le mot de passe, le numéro de port VNC, le chiffrement SSL et la valeur du délai d'attente. Il est possible de configurer ces paramètres à l'aide de RACADM ou de l'interface Web de l'iDRAC7.

REMARQUE : La fonction VNC est sous licence et est disponible sous la licence entreprise iDRAC7.

Vous pouvez choisir parmi plusieurs applications VNC ou clients bureau tels que ceux de RealVNC ou Dell Wyse PocketCloud.

Une seule session de client VNC peut être active à la fois.

Si la session VNC est active, vous pouvez uniquement lancer le média virtuel, et non la console virtuelle.

Si le cryptage vidéo est désactivé, le client VNC établit des liaisons RFB directement et les liaisons SSL sont inutiles. Pendant l'établissement des liaisons du client VNC (RFB ou SSL) si une autre session VNC est active ou si une session de console virtuelle est ouverte, la nouvelle session du client VNC est rejetée. Après l'achèvement de la phase initiale de l'établissement de liaisons, le serveur VNC désactive la console virtuelle et seul le média virtuel est autorisé. Une fois la session VNC terminée, le serveur VNC restaure l'état d'origine de la console virtuelle (activée ou désactivée).

Configuration de serveur VNC à l'aide de l'interface Web de l'iDRAC

Pour configurer les paramètres de serveur VNC :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → Services**.
   La page **Services** s'affiche.
2. Dans la section **Serveur VNC**, activez le serveur VNC, spécifiez le mot de passe, le numéro de port et l'activation ou la désactivation du cryptage SSL.
   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.
3. Cliquez sur **Appliquer**.
   Le serveur VNC est configuré.

Configuration du serveur VNC à l'aide de la RACADM

Pour configurer le serveur VNC, utilisez l'objet `VNCserver` avec la commande `set`. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC* disponible à l'adresse **dell.com/support/manuals**.

Configuration de l'écran du panneau avant

Vous pouvez configurer l'écran LCD du panneau avant et l'écran LED du système géré.

Pour les serveurs en rack ou de type tour, deux types de panneaux avant sont disponibles :

- Panneau avant LCD et LED d'identification du système
- Panneau avant LED et LED d'identification du système

Pour les serveurs lames, seul l'afficheur LED d'identification du système est disponible sur le panneau avant du serveur, car l'écran LCD se trouve sur le châssis de la lame.

Liens connexes

Configuration du paramétrage LCD
Configuration du paramétrage LED d'ID système

Configuration du paramétrage LCD

Vous pouvez définir et afficher une chaîne par défaut, telle que le nom, l'adresse IP d'iDRAC, etc. ou une chaîne que vous spécifier sur le panneau avant LCD du système géré.

Définition des paramètres de l'écran LCD en utilisant l'interface Web

Pour configurer l'écran LCD du panneau avant :

1. Dans l'interface Web d'iDRAC7, accédez)à **Présentation générale** → **Matériel** → **Panneau avant**.
2. Dans la section **Paramètres LCD**, dans le menu déroulant **Définir le message d'accueil**, sélectionnez les options suivantes :
   - numéro de service (valeur par défaut)
   - Asset Tag
   - Adresse MAC DRAC
   - Adresse IPv4 DRAC
   - Adresse IPv6 DRAC
   - Puissance système
   - Température ambiante
   - Modèle du système
   - Nom d'hôte
   - Défini par l'utilisateur
   - Aucun

     Si vous sélectionnez **Défini par l'utilisateur**, entrez le message approprié dans la zone de texte.

     Si vous sélectionnez **Aucun**, le message d'accueil ne s'affiche pas sur l'écran LCD du panneau avant du serveur.

3. Activer l'indication de la console virtuelle (facultatif). Si cette indication est activée, la section Alimentation du panneau avant actuelle et l'écran LCD du serveur affichent le message `Session de la console virtuelle active` lorsqu'une session de la console virtuelle est active.
4. Cliquez sur **Appliquer**.

   L'écran LCD affiche le message d'accueil défini.

Définition des paramètres LCD en utilisant l'interface RACADM

Pour configurer l'écran LCD du panneau avant, utilisez les objets dans le groupe **System.LCD**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Définition des paramètres de l'écran LCD en utilisant l'utilitaire de configuration d'iDRAC

Pour configurer l'écran LCD du panneau avant :

1. Dans l'utilitaire Paramètres iDRAC, allez sous **Sécurité du panneau avant**.

   La page **Sécurité du panneau avant des paramètres iDRAC** s'affiche
2. Activez ou désactivez le bouton d'alimentation.
3. Paramétrez les options suivantes :
   - Accès au panneau avant
   - Chaîne de messages LCD
   - Unités d'alimentation du système, unités de température ambiante, et affichage d'erreurs
4. Activez ou désactivez l'indication de la console virtuelle.

   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
5. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

Configuration du paramétrage LED d'ID système

Pour identifier un serveur, activez ou désactivez le clignotement du voyant d'identification du système sur le système géré.

Définition des paramètres LED d'identification du système en utilisant l'interface Web

Pour configurer l'afficheur LED d'identification du système :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Matériel** → **Panneau avant**. La page **Panneau avant** s'affiche.
2. Dans la section **Paramètres LED d'ID du système**, sélectionnez les options suivantes pour activer ou désactiver le clignotement LED :
   - Clignotement désactivé
   - Clignotement activé
   - Clignotement activé pour un jour
   - Clignotement activé pour un jour
   - Clignotement activé pour un jour
3. Cliquez sur **Appliquer**.

   Le clignotement LED est configuré sur le panneau avant.

Définition des paramètres LED d'identification du système à l'aide de l'interface RACADM

Pour configurer le voyant LED d'identification du système, utilisez la commande **setled**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration du fuseau horaire et NTP

Vous pouvez configurer le fuseau horaire sur iDRAC et synchroniser l'heure de l'iDRAC à l'aide du protocole NTP à la place des heures du BIOS ou du système hôte.

Vous devez disposer de privilèges de configuration pour configurer le fuseau horaire ou les paramètres de NTP.

Configuration du fuseau horaire et du protocole NTP à l'aide de l'interface Web iDRAC

Pour configurer le fuseau horaire et le NTP à l'aide de l'interface Web iDRAC :

1. Allez sous **Présentation** → **Paramètres iDRAC** → **Propriétés** → **Paramètres**.
   La page **Fuseau horaire et NTP** s'affiche.
2. Pour configurer le fuseau horaire, sélectionnez les fuseaux horaires requis dans le menu déroulant **Fuseau horaire**, puis cliquez sur **Appliquer**.
3. Pour configurer NTP, activez NTP, saisissez les adresses de serveur NTP, puis cliquez sur **Appliquer**.
   Pour plus d'informations sur les champs, voir l'*aide en ligne iDRAC7*.

Configuration du fuseau horaire et du protocole NTP à l'aide de RACADM

Pour configurer le fuseau horaire et le protocole NTP à l'aide de RACADM, utilisez les objets de **iDRAC.Time** et du groupe **iDRAC.NTPConfigGroup** avec la commande **set**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Définition du premier périphérique de démarrage

Vous pouvez définir le premier périphérique de démarrage ou du démarrage suivant uniquement ou pour tous les démarrages suivants. En fonction de cette sélection, vous pouvez définir le premier périphérique de démarrage du système. Le système démarre depuis le périphérique sélectionné lors du démarrage suivant et des démarrages ultérieurs et il reste le premier périphérique dans la séquence de démarrage du BIOS jusqu'à ce que vous le changiez dans l'interface Web d'iDRAC7 ou dans la séquence de démarrage du BIOS. Vous pouvez définir le premier périphérique de démarrage en effectuant l'une des actions suivantes :

- Démarrage normal
- PXE
- Configuration du BIOS
- Support amovible disquette/principal local
- CD/DVD local
- Disque dur
- Disquette virtuelle
- CD/DVD/ISO virtuel
- Carte SD locale

- vFlash
- Lifecycle Controller
- BIOS Boot Manager (Gestionnaire d'amorçage du BIOS)

REMARQUE :

- Le programme de configuration du BIOS (F2), Lifecycle Controller (F10), le gestionnaire d'amorçage du BIOS (F11) prennent uniquement en charge l'amorçage une fois activés.
- La console virtuelle ne prend pas en charge la configuration d'amorçage de manière permanente. Elle permet l'amorçage ponctuel.
- Les paramètres du premier périphérique de démarrage dans l'interface Web d'iDRAC7 remplacent les paramètres de démarrage du BIOS du système.

Définition du premier périphérique de démarrage en utilisant l'interface Web

Pour définir le premier périphérique de démarrage en utilisant l'interface Web :

1. Accédez à **Présentation générale → Serveur → Installation → Périphérique de démarrage initial**.
   L'écran **Périphérique de démarrage initial** s'affiche.
2. Sélectionnez le premier périphérique de démarrage dans la liste déroulante et cliquez sur **Appliquer**.
   Le système démarre depuis le périphérique sélectionné pour les démarrages suivants.
3. Pour démarrer depuis le périphérique une seule fois lors du démarrage suivant, sélectionnez **Boot Once** (Démarrer une seul fois). Ensuite, le système démarre depuis le premier périphérique de démarrage dans la séquence de démarrage du BIOS.
   Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC7*.

Définition du premier périphérique de démarrage à l'aide de l'interface RACADM

- Pour définir le premier périphérique de démarrage, utilisez l'objet **cfgServerFirstBootDevice**.
- Pour activer un seul démarrage pour un périphérique, utilisez l'objet **cfgServerBootOnce**.

Pour plus d'informations sur ces objets, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Définition du premier périphérique de démarrage à l'aide de la console virtuelle

Vous pouvez sélectionner le premier périphérique de démarrage alors que le serveur est affiché dans le visualiseur de la console virtuelle et avant que le serveur n'effectue sa séquence de démarrage. Vous pouvez effectuer un démarrage unique de tous les périphériques pris en charge répertoriés dans la liste Définition du premier périphérique de démarrage.

Pour définir le premier périphérique de démarrage à l'aide de la console virtuelle :

1. Lancer la console virtuelle
2. Dans le visualiseur de la console virtuelle, rendez-vous dans le menu **Démarrage suivant** et définissez le périphérique devant servir de premier périphérique de démarrage.

Activation du dernier écran de blocage

Pour identifier la cause du blocage du système, vous pouvez capturer l'image du blocage du système en utilisant iDRAC7.

Pour activer l'écran de blocage du système :

1. Depuis le DVD *Dell Systems Management Tools and Documentation*, installez Server Administrator sur le système géré.

   Pour plus d'informations, consultez le *Dell OpenManage Server Administrator Installation Guide*(Guide d'installation Dell OpenManage Server Administrator disponible sur le site) disponible à l'adresse **dell.com/support/manuals**.
2. Dans la fenêtre de démarrage et de récupération de **Windows**, vérifiez que l'option de redémarrage automatique n'est pas sélectionnée.

   Pour plus d'informations, voir la documentation de Windows.
3. Utilisez Server Administrator pour activer le minuteur de **récupération auto**, affectez à l'action de récupération automatique la valeur **Réinitialiser Mettre hors tension** ou **Cycle d'alimentation** et définissez les secondes pour le minuteur (valeur comprise entre 60 et 480).

   Pour plus d'informations, consultez le *Dell OpenManage Server Administrator Installation Guide*(Guide d'installation Dell OpenManage Server Administrator disponible sur le site) disponible à l'adresse **dell.com/support/manuals**.
4. Activez l'option **Arrêt et récupération automatiques** (ASR) en utilisant l'un des éléments suivants :
   - Server Administrator : voir le *Dell OpenManage Server Administrator User's Guide*(Guide d'utilisaton de Dell OpenManage Server Administrator disponible à l'adresse) disponible à l'adresse **dell.com/support/manuals**.
   - Interface locale RACADM — Utilisez la commande suivante :

     ```
     racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
     ```
5. Activez l'**agent de récupération de système automatique**. Pour ce faire, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau** → **Services**, sélectionnez **Activé** et cliquez sur **Appliquer**.

Activation ou désactivation de la connexion directe entre le SE et iDRAC

Dans les serveurs dotés d'une carte réseau fille (NDC) ou de périphériques LOM (LAN sur carte réseau), vous pouvez activer la fonction Connexion directe entre le SE et iDRAC qui fournit une communication haute vitesse bidirectionnelle intrabande entre l'iDRAC7 et le système d'exploitation hôte via un LOM partagé (serveurs en rack ou de type tour), une carte réseau dédiée (serveurs en rack, de type tour ou lame) ou la carte réseau USB. Cette fonction est disponible pour la licence iDRAC7 Enterprise.

Lorsque la fonction est activée via une carte réseau dédiée, vous pouvez lancer le navigateur dans le système d'exploitation hôte, puis accéder à l'interface Web iDRAC. La carte réseau dédiée pour les serveurs lame est accessible via le CMC.

Passer d'une carte réseau à l'autre ou d'un LOM partagé à l'autre ne nécessite aucun redémarrage ni aucune réinitialisation du système d'exploitation hôte ou de l'iDRAC.

Vous pouvez activer ce canal à l'aide de :

- l'interface Web iDRAC
- RACADM ou WS-MAN (environnement de système de post-exploitation).
- l'utilitaire Paramètres iDRAC(environnement de système de pré-exploitation)

Si la configuration réseau est modifiée via une interface Web iDRAC, vous devez patienter au moins 10 secondes avant d'activer la connexion directe entre le SE et l'iDRAC.

Si vous utilisez le fichier de configuration XML via RACADM ou WS-MAN et si les paramètres réseau sont modifiés dans ce fichier, vous devez alors patienter 15 secondes pour activer la fonction Connexion directe entre le SE et iDRAC ou définir l'adresse IP hôte du SE.

Avant d'activer la fonction Connexion directe entre le SE et iDRAC, assurez-vous que :

- L'iDRAC est configuré pour utiliser la carte NIC dédiée ou le mode partagé (c'est-à-dire, la sélection de carte NIC est assignée à l'un des périphériques LOM).
- Le système d'exploitation hôte et iDRAC7 se trouvent dans le même sous-réseau et le même VLAN.
- L'adresse IP du système d'exploitation hôte est configurée.
- Une carte qui prend en charge la fonction de transfert du SE à l'iDRAC est installée.
- Vous disposez du privilège de configuration.

Lorsque vous activez cette fonction :

- En mode partagé, l'adresse IP du système d'exploitation hôte est utilisée.
- En mode dédié, vous devez fournir une adresse IP valide pour le système d'exploitation hôte. Si plus d'un LOM est actif, saisissez l'adresse IP du premier LOM.

Une fois que vous avez activé la fonction Connexion directe entre le SE et iDRAC, si tout ne fonctionne pas correctement :

- Vérifiez que le câble NIC dédié de l'iDRAC est bien connecté.
- Assurez-vous qu'au moins un LOM est actif.

Liens connexes

Cartes prises en charge pour la connexion directe entre le système d'exploitation et l'iDRAC
Systèmes d'exploitation pris en charge pour la carte réseau USB
Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de l'interface Web
Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de RACADM
Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de l'utilitaire de configuration iDRAC

Cartes prises en charge pour la connexion directe entre le système d'exploitation et l'iDRAC

Le tableau suivant fournit une liste des cartes qui prennent en charge la fonction Connexion directe entre le SE et iDRAC à l'aide de LOM.

Tableau 8. : Connexion directe entre le SE et iDRAC à l'aide de LOM — Cartes prises en charge

Catégorie	Fabricant	Type
NDC	Broadcom	• 5720 QP rNDC 1 G BASE-T • 57810S DP bNDC KR • 57800S QP rNDC (10 G BASE-T + 1 G BASE-T) • 57800S QP rNDC (10 G SFP+ + 1 G BASE-T) • 57840 4x10G KR • rNDC 57840
	Intel	• i540 QP rNDC (10 G BASE-T + 1 G BASE-T) • i350 QP rNDC 1 G BASE-T • rNDC x520/i350 1 Go
	QLogic	QMD8262 NDC pour serveurs lame

Des cartes LOM intégrées prennent également en charge la fonction Connexion directe entre le système d'exploitation et l'iDRAC.

Les cartes suivantes ne prennent pas en charge la fonction Connexion directe entre le SE et iDRAC :

- NDC Intel 10 Go.
- Intel rNDC (Elk Flat rNDC) avec deux contrôleurs - Les contrôleurs 10 G ne sont pas pris en charge.
- Qlogic bNDC
- PCIe, mezzanine et cartes d'interface réseau.

Systèmes d'exploitation pris en charge pour la carte réseau USB

Les systèmes d'exploitation pris en charge pour la carte réseau USB sont les suivants :

- Windows Server 2008 SP2 (64 bits)
- Windows Server 2008 SP2 R2 (64 bits)
- Windows Server 2012 SP1
- SLES 10 SP4 (64 bits)
- SLES 11 SP2 (64 bits)
- RHEL 5.9 (32 bits et 64 bits)
- RHEL 6.4
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U1 ESXi
- vSphere v5.5 ESXi

Sur les serveurs dotés de Windows 2008 SP2 64 bits, le périphérique USB CD virtuel iDRAC n'est pas détecté automatiquement (ou activé). Vous devez l'activer manuellement. Pour plus d'informations, voir les étapes recommandées par Microsoft pour mettre à jour manuellement le pilote Remote Network Driver Interface Specification (RNDIS) de ce périphérique.

Pour les systèmes d'exploitation Linux, configurez la carte réseau USB comme le protocole DHCP sur le système d'exploitation de l'hôte avant d'activer la carte réseau USB.

Si le système d'exploitation hôte est SUSE Linux Enterprise Server 11, après l'activation de la carte réseau USB sur l'iDRAC, vous devez activer manuellement le client DHCP sur le système d'exploitation hôte. Pour des informations sur l'activation de DHCP, voir les documents portant sur les systèmes d'exploitation SUSE Linux Enterprise Server 11.

Pour vSphere, vous devez installer le fichier VIB avant d'activer la carte réseau USB.

Pour les systèmes d'exploitation suivants, si vous installez les progiciels Avahi et nss-mdns, vous pouvez alors utiliser **https://idrac.local** pour lancer l'iDRAC à partir du système d'exploitation hôte. Si ces modules ne sont pas installés, utilisez **https://169.254.0.1** pour lancer l'iDRAC.

Système d'exploitation	État du pare-feu	Progiciel Avahi	Progiciel nss-mdns
RHEL 5.9 32 bits	Désactiver	Installez séparément (**avahi-0.6.16-10.el5_6.i386.rpm**)	Installez séparément (**nss-mdns-0.10-4.el5.i386.rpm**)
RHEL 6.4 64 bits	Désactiver	Installez séparément (**avahi-0.6.25-12.el6.x86_64.rpm**)	Installez séparément (**nss-mdns-0.10-8.el6.x86_64.rpm**)
SLES 11 SP3 64 bits	Désactiver	Le progiciel Avahi fait partie du DVD du système d'exploitation	nss-mdns est installé lors de l'installation d'Avahi

Sur le système hôte, lors de l'installation du système d'exploitation RHEL 5.9, le mode de connexion directe de la carte réseau USB est en état désactivé. S'il est activé une fois l'installation terminée, l'interface réseau correspondant au périphérique de carte réseau USB n'est pas active automatiquement. Vous pouvez effectuer l'une des opérations suivantes pour activer le périphérique de carte réseau USB :

- Configurez l'interface de la carte réseau USB à l'aide de l'outil Network Manager. Naviguez vers **Système** → **Administrateur** → **Réseau** → **Périphériques** → **Nouveau** → **Connexion Ethernet** et sélectionnez **Dell computer corp.Périphérique USB virtuel de carte réseau iDRAC**. Cliquez sur l'icône Activation pour activer le périphérique. Pour plus d'informations, voir la documentation RHEL 5.9.
- Créer un fichier de configuration de l'interface correspondante appelé **ifcfg-ethX** dans le répertoire **/etc/sysconfig/network-script/**. Ajoutez les entrées de base DEVICE, BOOTPROTO, HWADDR, ONBOOT. Ajoutez le TYPE au fichier **ifcfg-ethX** et redémarrez les services réseau à l'aide de la commande `service network restart`.
- Redémarrez le système.
- Éteignez et mettez le système sous tension.

Sur les systèmes équipés du système d'exploitation RHEL 5.9, si la carte réseau USB a été désactivée et si vous éteignez le système ou vice versa, lorsque le système est mis sous tension et si la carte réseau USB est activée, le périphérique de carte réseau USB n'est pas actif automatiquement. Pour l'activer, vérifiez si un fichier **ifcfg-ethX.bak** est disponible dans le répertoire **/etc/sysconfig/network-script** pour l'interface de carte réseau USB. S'il est disponible, renommez-le **ifcfg-ethX**, puis utilisez la commande `ifup ethX`.

Liens connexes

Installation des fichiers VIB

Installation des fichiers VIB

Pour les systèmes d'exploitation vSphere, avant d'activer la carte réseau USB, vous devez installer le fichier VIB.

Pour installer le fichier VIB :

1. À l'aide de Win-SCP, copiez le fichier VIB vers le dossier **/tmp/** du système d'exploitation hôte ESX -i.
2. Allez sur l'invite ESXi et exécutez la commande suivante :

   ```
   esxcli software vib install -v /tmp/ iDRAC_USB_NIC-1.0,0-799733X03.vib --no-sig-check
   ```

   Le résultat est :

   ```
   Message : The update completed successfully, but the system needs to be rebooted for the changes to be effective. Reboot Required: true VIBs Installed: Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03 VIBs Removed: VIBs Skipped:
   ```
3. Redémarrez le serveur.
4. À l'invite ESXi, exécutez la commande : `esxcfg-vmknic l`.

   Le résultat affiche l'entrée usb0.

Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de l'interface Web

Pour activer la connexion directe entre le SE et iDRAC à l'aide de l'interface Web :

1. Allez sous **Présentation** → **Paramètres iDRAC** → **Réseau** → **Connexion directe entre le SE et iDRAC**.

   La page **Connexion directe entre le SE et iDRAC** s'affiche.
2. Sélectionnez l'une des options suivantes pour activer la connexion directe entre le système d'exploitation et l'iDRAC :

   – **LOM** : le lien de transfert du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le périphérique LOM ou NDC.

   – **USB** : le lien de transfert du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le bus USB interne.

   Pour désactiver cette fonction, sélectionnez **Désactivé**.

3. Si vous sélectionnez **LOM** en tant que configuration de transfert, et que le serveur est connecté à l'aide du mode dédié, saisissez l'adresse IPv4 du système d'exploitation. La valeur par défaut est 0.0.0.0.

   REMARQUE : Si le serveur est connecté en mode LOM partagé, le champ **Adresse IP du SE** est désactivé.

4. Si vous choisissez **Carte réseau USB** comme configuration de connexion directe, entrez l'adresse IP de la carte réseau USB. La valeur par défaut est 169.254.0.1. Il est recommandé d'utiliser l'adresse IP par défaut. Toutefois, si cette adresse IP entre en conflit avec une adresse IP d'autres interfaces du système hôte ou du réseau local, vous devez la modifier.

5. Cliquez sur **Appliquer** pour appliquer les paramètres.

6. Cliquez sur **Configuration réseau test** pour vérifier si l'IP est accessible et si le lien est établi entre l'iDRAC et le système d'exploitation hôte.

Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de RACADM

Pour activer ou désactiver la fonction Connexion directe entre le SE et iDRAC à l'aide de RACADM, utilisez les objets du groupe **iDRAC.OS-BMC**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de l'utilitaire de configuration iDRAC

Pour activer ou désactiver l'option Connexion directe entre le SE et iDRAC à l'aide de l'utilitaire de configuration iDRAC :

1. Dans l'utilitaire de configuration iDRAC, allez sous **Connexion directe entre le SE et iDRAC**.

   La page **Configuration iDRAC - Connexion directe entre le SE et iDRAC** s'affiche.

2. Sélectionnez l'une des options suivantes pour activer la connextion directe entre le système d'exploitation et l'iDRAC :

   - **LOM** : le lien de transfert du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le périphérique LOM ou NDC.
   - **USB** : le lien de transfert du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le bus USB interne.

   Pour désactiver cette fonction sélectionnez **Désactivée**.

3. Si vous sélectionnez **LOM** en tant que configuration de transfert, et que le serveur est connecté à l'aide du mode dédié, saisissez l'adresse IPv4 du système d'exploitation. La valeur par défaut est 0.0.0.0.

   REMARQUE : Si le serveur est connecté en mode LOM partagé, le champ **Adresse IP du SE** est désactivé.

4. Si vous choisissez **Carte réseau USB** comme configuration de connexion directe, entrez l'adresse IP de la carte réseau USB.

   La valeur par défaut est 169.254.0.1. Toutefois, si cette adresse IP en conflit avec une adresse IP d'autres interfaces du système hôte ou duréseau local, vous devez la modifier.

5. Cliquez sur **Retour**, **Terminer**, puis **Oui**. Les paramètres sont enregistrés.

Obtention de certificats

Le tableau suivant répertorie les types de certificats en fonction du type de connexion.

Tableau 9. Types de certificats en fonction du type de connexion

Type de connexion	Type de certificat	Mode d'obtention
Connexion directe en utilisant Active Directory	Certificat CA de confiance	Générer un fichier RSC et le faire signer par une autorité de certification Les certificats SHA-2 sont également pris en charge.
Connexion avec une carte à puce comme utilisateur local ou Active Directory	• Certificat utilisateur • Certificat CA de confiance	• Certificat utilisateur : exportez le certificat utilisateur de carte à puce comme fichier codé en base 64 en utilisant le logiciel de gestion de carte fourni par le fournisseur de carte à puce. • Certificat CA de confiance : ce certificat est émis par une autorité de certification. Les certificats SHA-2 sont également pris en charge.
Connexion utilisateur Active Directory	Certificat CA de confiance	Ce certificat est émis par une autorité de certification. Les certificats SHA-2 sont également pris en charge.
Connexion d'utilisateur local	Certificat SSL	Générer un fichier RSC et le faire signer par une autorité de certification de confiance **REMARQUE :** iDRAC7 est fourni avec un certificat de serveur SSL autosigné par défaut. Le serveur Web iDRAC7, Média Virtuel et la console virtuelle utilisent ce certificat. Les certificats SHA-2 sont également pris en charge.

Liens connexes

Certificats de serveur SSL
Génération d'une nouvelle demande de signature de certificat

Certificats de serveur SSL

iDRAC7 inclut un serveur Web configuré pour utiliser le protocole de sécurité standard SSL pour transférer des données cryptées dans un réseau. SSL, qui repose sur une technologie de cryptage asymétrique, est largement utilisé dans les communications authentifiées et cryptées entre les clients et les serveurs pour empêcher l'écoute sur un réseau.

Un système SSL peut effectuer les tâches suivantes :

- S'authentifier auprès d'un client SSL
- Permettre aux deux systèmes d'établir une connexion cryptée

Le processus de cryptage fournit un haut niveau de protection de données. iDRAC7 utilise le cryptage SSL 1 289 bits, à savoir la forme de cryptage la plus sûre généralement disponible pour les navigateurs Web en Amérique du nord.

Le serveur Web iDRAC7 possède un certificat numérique SSL unique auto-signé Dell par défaut. Vous pouvez remplacer ce certificat SSL par défaut par un certificat signé par une autorité de certification (CA) connue. Une autorité de

certification est une entité commerciale reconnue dans l'industrie de la technologie informatique pour répondre de manière fiable aux normes exigeantes en matière de filtrage, d'identification et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples de CA. Pour initialiser le processus d'obtention d'un certificat signé par une autorité de certification, utilisez l'interface Web iDRAC7 ou l'interface RACADM pour générer une Requête de signature de certificat (RSC), accompagnée des informations sur votre société. Soumettez ensuite la RSC générée à une CA telle que VeriSign ou Thawte. Le CA peut être un CA racine ou intermédiaire. Une fois que vous avez reçu le certificat SSL signé par une CA, chargez-le sur iDRAC.

Le certificat SSL de chaque iDRAC que la station de gestion doit approuver doit être placé dans le magasin de certificats de la station de gestion. Une fois le certificat SSL installé sur les stations de gestion, les navigateurs pris en charge peuvent accéder à iDRAC sans renvoyer d'avertissements de certificat.

Vous pouvez également téléverser un certificat de signature personnalisé pour signer le certificat SSL, au lieu de compter sur le certificat de signature par défaut pour cette fonction. En important un certificat de signature personnalisé dans toutes les stations de gestion, tous les iDRAC utilisant le certificat de signature personnalisé sont approuvés. Si un certificat de signature personnalisé est téléversé alors qu'un certificat SSL personnalisé est utilisé, le certificat SSL personnalisé est désactivé et un certificat unique SSL auto-généré signé par le certificat de signature personnalisé est utilisé. Vous pouvez télécharger le certificat de signature personnalisé (sans clé privée). Vous pouvez également supprimer un certificat de signature personnalisé existant. Après avoir supprimé le certificat de signature personnalisé, iDRAC résinitialise et auto-génère un nouveau certificat SSL auto-signé. Si un certificat auto-signé est regénéré, l'iDRAC doit de nouveau être approuvé par la station de gestion. Les certificats SSL auto-générés sont auto-signés et expirent après sept ans et un jour, leur date de démarrage enregistrée comme étant un jour plus tôt (pour les différentes configurations de fuseau horaire des stations de gestion et de l'iDRAC).

Le certificat SSL de serveur Web de l'iDRAC7 prend en charge le caractère astérisque (*) comme une partie du composant le plus à gauche du nom commun lors de la génération d'une requête de signature de certificat (RSC). Par exemple,*.qa.com ou*.company.qa.com. Cela s'appelle un certificat générique. Si une RSC générique est générée à l'extérieur de l'iDRAC, celle-ci est équipée d'un seul certificat SSL générique signé que vous pouvez charger pour plusieurs iDRAC et toutes les iDRAC sont considérées comme fiables par les navigateurs pris en charge. En se connectant à l'interface Web iDRAC à l'aide d'un navigateur pris en charge qui prend en charge un certificat générique, l'iDRAC est considérée comme fiable par le navigateur. Tout en lançant des visionneuses, les contrôleurs iDRAC sont considérés comme fiables par le visualiseur des clients.

Liens connexes

- Génération d'une nouvelle demande de signature de certificat
- Téléversement d'un certificat d'un serveur
- Affichage du certificat de serveur
- Téléversement d'un certificat de signature personnalisée
- Télécharger un certificat de signature de certificat SSL personnalisé
- Suppression d'un certificat de signature de certificat SSL personnalisé

Génération d'une nouvelle demande de signature de certificat

Une demande RSC est une demande numérique envoyée à une autorité de certification pour obtenir un certificat de serveur SSL. Les certificats de serveur SSL permettent aux clients de faire confiance à l'identité du serveur et de négocier une session cryptée avec le serveur.

Lorsque l'autorité de certification reçoit une demande RSC, elle vérifie les informations que contient la demande. Si le demandeur répond aux critères de l'autorité de certification, cette dernière émet un certificat de serveur SSL avec une signature numérique qui identifie de manière unique le serveur lorsqu'il établit des connexions SSL avec les navigateurs exécutés sur les stations de gestion

Lorsque l'autorité de certification accepte la demande RSC et émet le certificat de serveur SSL, ce dernier peut être téléversé vers iDRAC7. Les informations utilisées pour générer la demande RSC, stockées dans le micrologiciel

d'iDRAC7, doivent correspondre aux informations contenues dans le certificat de serveur SSL, à savoir que le certificat doit avoir été généré en utilisant la demande RSC créée par iDRAC7.

Liens connexes

Certificats de serveur SSL

Génération d'un fichier RSC en utilisant l'interface Web

Pour générer un fichier RSC :

REMARQUE : Chaque nouveau fichier RSC remplace les données RSC stockées dans le micrologiciel. Les informations dans le fichier RSC doivent correspondre aux informations dans le certificat de serveur SSL. Autrement, iDRAC7 n'accepte pas le certificat.

1. Dans l'interface Web d'iDRAC, accédez à **Présentation générale → Paramètres iDRAC → Réseau → SSL**, sélectionnez **Générer une nouvelle demande de signature de certificat (CSR)** et cliquez sur **Suivant**.

   La page **Générer une nouvelle demande de signature de certificat** s'affiche.
2. Entrez une valeur pour chaque attribut RSC.

   Reportez-vous à *l'aide en ligne d'IDRAC7* pour plus d'informations.
3. Cliquez sur **Générer**.

   Un nouveau fichier CSR est généré. Enregistrez-le sur la station de gestion.

Génération d'un fichier RSC à l'aide de l'interface RACADM

Pour générer une CSR à l'aide de RACADM, utilisez les objets du groupe **cfgRacSecurity** avec la commande **config** ou utilisez les objets du groupe **iDRAC.Security** avec la commande **set**, puis utilisez la commande **sslcsrgen** pour générer la CSR. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Téléversement d'un certificat d'un serveur

Après avoir généré une RSC, vous pouvez charger le certificat de serveur SSL vers le micrologiciel iDRAC7. L'iDRAC7 se réinitialise une fois le certificat chargé. L'iDRAC7 accepte uniquement les certificats de serveur Web X509 codés en Base 64.

PRÉCAUTION : iDRAC7 devient indisponible pendant quelques minutes lors de l'initialisation.

Liens connexes

Certificats de serveur SSL

Téléversement d'un certificat de serveur en utilisant l'interface Web

Pour téléverser un certificat de serveur SSL :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → SSL**, sélectionnez **Upload Server Certificate** (Téléverser un certificat de serveur) et cliquez sur **Suivant**.

   L'écran **Téléversement du certificat** s'affiche.
2. Sous **Chemin du fichier**, cliquez sur **Parcourir** et sélectionnez le certificat sur la station de gestion.
3. Cliquez sur **Apply** (Appliquer).

   Le certificat de serveur SSL est téléversé vers le micrologiciel d'iDRAC7 et remplace le certificat existant..

Téléversement d'un certificat de serveur à l'aide de l'interface RACADM

Pour téléverser le certificat de serveur SSL, utilisez la commande **sslcertupload**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible à l'adresse **dell.com/support/manuals**.

Si la RSC est générée à l'extérieur d'iDRAC avec une clé privée disponible, puis pour téléverser le certificat sur l'iDRAC :

1. Envoyez la RSC à une autorité de certification racine connue. L'autorité de certification signe la RSC, qui devient un certificat valide.
2. Téléversez la clé privée à l'aide de la commande racadm `sslkeyupload` à distance.
3. Téléversez le certificat signé sur l'iDRAC à l'aide de la commande racadm `sslcertupload` à distance.

   L'iDRAC redémarre et le certificat récemment téléversé prend effet.

Affichage du certificat de serveur

Vous pouvez afficher le certificat de serveur SSL actuel utilisé dans iDRAC7.

Liens connexes

Certificats de serveur SSL

Affichage d'un certificat de serveur à l'aide de l'interface Web

Dans l'interface Web iDRAC7, allez sous **Présentation → Paramètres iDRAC → Réseau → SSL**. Le certificat de serveur SSL en cours d'utilisation s'affiche en haut de la page **SSL**.

Affichage d'un certificat de serveur à l'aide de l'interface RACADM

Pour afficher le certificat de serveur SSL, utilisez la commande **sslcertview**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Téléversement d'un certificat de signature personnalisée

Vous pouvez téléverser un certificat à signature personnalisée pour signer le certificat SSL. Les certificats SHA-2 sont également pris en charge.

Téléversement d'un certificat de signature personnalisé à l'aide de l'interface Web

Pour téléverser un certificat de signature personnalisé à l'aide de l'interface Web d'iDRAC7 :

1. Allez dans **Présentation → Paramètres iDRAC → Réseau → SSL**.

   La page **SSL** s'affiche.
2. Sous **Certificat de signature de certificat SSL personnalisé**, sélectionnez **Téléverser le certificat de signature de certificat SSL personnalisé**, puis cliquez sur **Suivant**.

   La page **Téléverser le certificat de signature de certificat SSL personnalisé** s'affiche.
3. Cliquez sur **Parcourir** et sélectionnez le certificat de signature de certificat SSL personnalisé.

   Seul le certificat PKCS #12 (Public-Key Cryptography Standards #12 - Chiffrement de clé publique de norme n° 12) est pris en charge.
4. Si le certificat est protégé par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe du certificat PKCS#12**.

5. Cliquez sur **Appliquer**.

   Le certificat est téléversé sur iDRAC et iDRAC se réinitialise. L'iDRAC devient non disponible pendant quelques minutes lors de la réinitialisation.

Téléversement d'un certificat de signature de certificat SSL personnalisé à l'aide de RACADM

Pour téléverser le certificat de signature de certificat SSL personnalisé à l'aide de racadm, utilisez la sous-commande **sslcertupload**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Télécharger un certificat de signature de certificat SSL personnalisé

Vous pouvez télécharger le certificat de signature personnalisé à l'aide de l'interface Web iDRAC7 ou RACADM.

Téléchargement du certificat de signature personnalisé

Pour télécharger le certificat de signature personnalisé à l'aide de l'interface Web d'iDRAC7 :

1. Allez dans **Présentation → Paramètres iDRAC → Réseau → SSL**.

   La page **SSL** s'affiche.
2. Sous **Certificat de signature de certificat SSL personnalisé**, sélectionnez **Télécharger le certificat de signature de certificat SSL personnalisé**, puis cliquez sur **Suivant**.

   Un message contextuel s'affiche vous permettant d'enregistrer le certificat de signature personnalisé sur un emplacement de votre choix.

Téléchargement d'un certificat de signature de certificat SSL personnalisé à l'aide de RACADM

Pour télécharger le certificat de signature de certificat SSL personnalisé à l'aide de racadm, utilisez la sous-commande **sslcertdownload**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Suppression d'un certificat de signature de certificat SSL personnalisé

Vous pouvez également supprimer un certificat de signature personnalisé existant à l'aide de l'interface Web iDRAC7 ou de RACADM.

Suppression d'un certificat de signature personnalisé

Pour supprimer un certificat de signature personnalisé à l'aide de l'interface Web d'iDRAC7 :

1. Allez dans **Présentation → Paramètres iDRAC → Réseau → SSL**.

   La page **SSL** s'affiche.
2. Sous **Certificat de signature de certificat SSL personnalisé**, sélectionnez **Supprimer le certificat de signature de certificat SSL personnalisé**, puis cliquez sur **Suivant**.

   Le certificat de signature personnalisé est supprimé de l'iDRAC. L'iDRAC se réinitialise et revient au certificat SSL auto-signé par défaut auto-généré par le serveur Web. iDRAC devient indisponible lors de la réinitialisation.

Suppression d'un certificat de signature de certificat SSL personnalisé à l'aide de RACADM

Pour supprimer le certificat de signature de certificat SSL personnalisé à l'aide de RACADM, utilisez la sous-commande **sslcertdelete**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration de plusieurs iDRAC7 en utilisant l'interface RACADM

Vous pouvez configurer plusieurs iDRAC7 avec des propriétés identiques en utilisant l'interface RACADM. Lorsque vous interrogez un iDRAC7 en utilisant son ID de groupe et son ID d'objet, l'interface RACADM crée le fichier de configuration **.cfg** depuis les informations extraites. Vous définissez le nom du fichier. Importez le fichier vers les autres iDRAC7 pour les configurer à l'identique.

REMARQUE : Quelques fichiers de configuration contiennent des informations iDRAC7 uniques (telles que l'adresse IP fixe) que vous devez modifier avant d'exporter le fichier vers les autres iDRAC7.

Vous pouvez également utiliser le fichier XML de configuration système pour configurer plusieurs iDRAC à l'aide de RACADM. Le fichier XML de configuration système contient les informations relatives à la configuration des composants, et ce fichier est utilisé pour appliquer la configuration au BIOS, à l'iDRAC, RAID, et à la carte réseau en important le fichier dans un système cible. Pour en savoir plus, consultez le document technique *Flux de travail de la configuration XML* disponible à l'adresse **dell.com/support/manuals** ou dans le centre technique Dell.

Pour configurer plusieurs iDRAC7 à l'aide du fichier **.cfg** :

1. Interrogez l'iDRAC7 cible qui contient la configuration nécessaire en utilisant la commande `racadm getconfig -f monfichier.cfg`.

   La commande demande la configuration iDRAC7 et génère le fichier **myfile.cfg**. Si nécessaire, vous pouvez configurer le fichier avec un autre nom.

   REMARQUE : La redirection d'une configuration iDRAC7 vers un fichier à l'aide de `getconfig-f` est seulement prise en charge avec les interfaces RACADM locale et distante.

   REMARQUE : Le fichier .cfg généré ne contient pas de mots de passe utilisateur.

   La commande **getconfig** affiche toutes les propriétés de configuration dans un groupe (défini par un nom de groupe et un index) et toutes les propriétés de configuration d'un utilisateur en fonction du nom d'utilisateur.
2. Modifiez le fichier de configuration à l'aide d'un simple éditeur de texte (facultatif).

   REMARQUE : Il est recommandé de modifier ce fichier avec un simple éditeur de texte. L'utilitaire RACADM utilise un analyseur de texte ASCII. Le formatage risque de perturber l'analyseur et de corrompre la base de données RACADM.
3. Utilisez le nouveau fichier de configuration pour modifier la cible iDRAC7 en utilisant la commande `racadm config -f monfichier.cfg`

   La commande charge les informations vers l'autre iDRAC7. Vous pouvez utiliser la sous-commande **config** pour synchroniser la base de données des utilisateurs et des mots de passe avec Server Administrator.
4. Réinitialisez la cible iDRAC7 en utilisant la commande `racadm racreset`

Création d'un fichier de configuration iDRAC7

Le fichier de configuration **.cfg** peut être :

- Créé
- Obtenu depuis la commande `racadm getconfig -f <nom_de_fichier>.cfg` ou la commande `racadm get -f <nom_de_fichier>.cfg`
- Obtenu depuis la commande `racadm getconfig -f <nom_de_fichier>.cfg` ou la commande `racadm get -f <nom_de_fichier>.cfg`

  Pour en savoir plus sur les commandes **getconfig** et **get**, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) est disponible à l'adresse **dell.com/support/manuals** .

Le fichier **.cfg** est le premier analysé pour vérifier que le groupe et les noms d'objets valides sont présents et que les règles de syntaxe de base sont respectées. Les erreurs sont indiquées par le numéro de ligne de l'erreur et un message explique le problème. L'ensemble du fichier est analysé pour déterminer les erreurs éventuelles et toutes les erreurs détectées sont affichées. Les commandes d'écriture ne sont pas envoyées à iDRAC7 si une erreur est détectée dans le fichier **.cfg**. L'utilisateur doit éliminer toutes les erreurs avant d'utiliser le fichier pour configurer iDRAC7. Utilisez l'option `-c` dans la sous-commande `config` pour vérifier la syntaxe ; cette sous-commande n'exécute pas d'opération d'écriture vers iDRAC7.

Suivez les instructions ci-dessous lorsque vous créez un fichier **.cfg** :

- Si l'analyseur détecte un groupe indexé, l'index du groupe est utilisé comme ancre. Les modifications apportées aux objets dans le groupe indexé sont également associées à la valeur d'index.

  Par exemple :

  – Si vous avez utilisé la commande **getconfig** :

  ```
  [cfgUserAdmin] # cfgUserAdminIndex=11 cfgUserAdminUserName= #
  cfgUserAdminPassword=******** (Write-Only) cfgUserAdminEnable=0
  cfgUserAdminPrivilege=0x00000000 cfgUserAdminIpmiLanPrivilege=15
  cfgUserAdminIpmiSerialPrivilege=15 cfgUserAdminSolEnable=0
  ```

  – Si vous avez utilisé la commande **get** :

  ```
  [idrac.users.16] Enable=Disabled IpmiLanPrivilege=15
  IpmiSerialPrivilege=15 !!Password=******** (Write-Only) Privilege=0x0
  SNMPv3AuthenticationType=SHA SNMPv3Enable=Disabled SNMPv3PrivacyType=AES
  SolEnable=Disabled UserName=
  ```

- Les index sont en lecture seule et ne peuvent pas être modifiés. Les objets du groupe indexé sont liés sous l'index où ils se trouvent et toute configuration valide pour la valeur d'objet est applicable uniquement à cet index.
- Un groupe d'index prédéfinis est disponible pour chaque groupe indexé. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals** .
- Utilisez la sous-commande `racresetcfg` pour restaurer les paramètres par défaut définis en usine d'iDRAC7, puis exécutez la commande `racadm config -f <nom_du_fichier>.cfg` ou `racadm set -f <nom_du_fichier>.cfg`. Assurez-vous que le fichier **.cfg** inclus tous les objets, utilisateurs, index ou autres paramètres requis.

PRÉCAUTION : Utilisez la sous-commande `racresetcfg` pour restaurer les paramètres par défaut de la base de données et de la carte réseau iDRAC7, et pour supprimer tous les utilisateurs et configurations d'utilisateurs. Bien que l'utilisateur root soit disponible, d'autres paramètres utilisateur par défaut sont également restaurés.

Règles d'analyse

- Toutes les lignes qui commencent par '#' sont considérées correspondre à des commentaires. Une ligne de commentaire doit commencer dans la colonne 1. Le caractère '#' dans les autres colonnes est traité comme un caractère '#'. Certains paramètres de modem peuvent contenir des caractères #. Aucun caractère d'échappement n'est nécessaire. Vous pouvez générer un fichier **.cfg** depuis une commande `racadm getconfig -f <nom de fichier> .cfg` et exécuter la commande `racadm config -f <nom de fichier> .cfg` dans un iDRAC7 différent sans ajouter de caractères d'échappement. Exemple :

  ```
  #
  # Il s'agit d'un commentaire
  [cfgUserAdmin]
  cfgUserAdminPageModemInitString=<Modem init # n'est pas un commentaire>
  ```

- Toutes les entrées de groupe doivent être placées entre « `[` » et « `]` ». Le premier caractère « `[` » représentant un nom de groupe *doit* commencer dans la colonne 1. Ce nom de groupe *doit* être défini avant les objets du groupe. Les objets qui ne contiennent pas de nom de groupe associé génèrent une erreur. Les données de configuration sont organisées comme indiqué dans le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**. L'exemple suivant montre un nom de groupe, un objet et la valeur de propriété de l'objet.

```
[cfgLanNetworking] - {nom de groupe}
cfgNicIpAddress=143.154.133.121 {nom d'objet}
```

- Tous les paramètres sont spécifiés en tant que paires « objet=valeur » sans espace entre l'objet, le signe = et la valeur.

  Les espaces inclus après la valeur sont ignorés. Un espace dans une chaîne de valeur ne change pas. Les caractères à droite de «=»' sont utilisés tels quels (par exemple, un second «=» ou un «#», « [', '] », etc.). Ces caractères sont des caractères de script de discussion de modem valides.

  Voir l'exemple de la puce précédente.

  La commande `racadm getconfig-f <nom de fichier>.cfg` place un commentaire devant les objets d'index, ce qui permet à l'utilisateur de voir les commentaires inclus.

  Pour voir le contenu d'un groupe indexé, utilisez la commande suivante :

  ```
  racadm getconfig -g <nom de groupe> -i <index 1-16>
  ```

- Pour les groupes indexés, l'objet Anchor doit être le premier objet après la paire « [ ] ». Voici des exemples des groupes indexés actuels :

  ```
  [cfgUserAdmin]
  cfgUserAdminIndex=11
  ```

  Si vous tapez `racadm getconfig -f <`*monexemple*`>.cfg`, la commande génère un fichier **.cfg** pour la configuration iDRAC7 actuelle. Ce fichier de configuration peut être utilisé comme exemple et comme modèle pour votre propre fichier . **cfg**.

Modification de l'adresse IP d'iDRAC7

Lorsque vous modifiez l'adresse IP d'iDRAC7 dans le fichier de configuration, supprimez toutes les entrées *<variable>*=**value** inutiles. Seule l'étiquette avec « [" et "] » du groupe de variables reste, y compris les deux entrées *<variable>*=**value** qui appartiennent à la modification d'adresse IP.

Par exemple :

```
#
# Groupe d'objets "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#
# Groupe d'objets "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# commentaire, le reste de cette ligne est ignoré
cfgNicGateway=10.35.9.1
```

La commande `racadm config -f myfile.cfg` analyse le fichier et identifie les erreurs sur chaque ligne. Un fichier correct met à jour les entrées appropriées. En outre, vous pouvez utiliser la commande `getconfig` de l'exemple précédent pour vérifier la mise à jour.

Utilisez ce fichier pour télécharger des modifications à l'échelle de la société ou pour configurer de nouveaux systèmes sur le réseau.

REMARQUE : « Ancre » est un terme interne ; ne l'utilisez pas dans le fichier

Désactivation de l'accès pour modifier les paramètres de configuration iDRAC7 sur un système hôte

Vous pouvez désactiver l'accès pour modifier les paramètres de configuration iDRAC7 via l'interface locale RACADM ou l'utilitaire de configuration d'iDRAC. Cependant, vous pouvez afficher ces paramètres de configuration. Pour ce faire :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau** → **Services**.
2. Sélectionnez l'une des options suivantes ou les deux :
   - **Désactiver la configuration local iDRAC à l'aide des paramètres iDRAC** — Désactive l'accès pour modifier les paramètres de configuration dans l'utilitaire de configuration iDRAC.
   - **Désactiver la configuration locale iDRAC à l'aide de l'interface RACADM** — Désactive l'accès pour modifier les paramètres de configuration dans l'interface locale RACADM.
3. Cliquez sur **Appliquer**.

   REMARQUE : Si l'accès est désactivé, vous ne pouvez pas utiliser Server Administrator ni IPMITool pour exécuter les configurations iDRAC7. Cependant, vous pouvez utiliser IPMI sur le LAN.

5

Affichage des informations iDRAC7 et d'un système géré

Vous pouvez afficher l'intégrité et les propriétés d'iDRAC7 et d'un système géré, l'inventaire matériel et logiciel, l'intégrité des capteurs, les périphériques de stockage, les périphériques réseau et afficher les sessions utilisateur et y mettre fin. Pour les serveurs lames, vous pouvez également afficher les informations FlexAddress.

Liens connexes

Affichage de l'intégrité et des propriétés d'un système géré

Lorsque vous ouvrez une session dans l'interface Web d'iDRAC7, la page du **résumé du système** permet de visualiser l'intégrité du système et les informations iDRAC7 de base, de prévisualiser la console virtuelle, d'ajouter et de visualiser des notes de travail et de lancer rapidement des tâches, telles que la mise sous tension ou hors tension, un cycle d'alimentation, l'affichage de journaux, la mise à jour et la restauration du micrologiciel, la mise sous ou hors tension des DEL du panneau avant et la réinitialisation de l'iDRAC7.

Pour accéder à la page du **résumé du système**, accédez à **Présentation générale → Serveur → Propriétés → Résumé**. La page du **résumé du système** s'affiche. Pour plus d'informations, voir l'*aide en ligne d'iDRAC7*.

Vous pouvez également afficher les informations de base du résumé du système en utilisant l'utilitaire de configuration d'iDRAC. Pour ce faire, dans l'utilitaire Paramètres iDRAC, accédez à **Résumé du système**. La page **Résumé du système - Paramètres d'iDRAC** s'affiche. Pour plus d'informations, voir l'*aide en ligne de l'utilitaire Paramètres iDRAC*.

Affichage de l'inventaire du système

Vous pouvez afficher des informations sur les composants matériels et logiciels installés sur le système géré. Pour ce faire, dans l'interface Web d'iDRAC7, accédez à **Overview → Server → Properties → System Inventory** (Présentation générale, Serveur, Propriétés, Résumé du système). Pour visualiser des informations sur les propriétés affichées, voir l'*aide en ligne d'iDRAC7*.

La section Inventaire de matériel affiche les informations sur les composants suivants disponibles sur le système géré :

- iDRAC
- Contrôleur RAID

- Batteries
- UC
- Barrettes de mémoire DIMM
- Disque durs
- Fonds de panier
- Cartes d'interface réseau (incorporées et intégrées)
- Carte vidéo
- la carte SD
- Unité d'alimentation (PSU)
- Ventilateurs
- HBA Fibre Channel
- USB

La section Inventaire de micrologiel affiche la version de micrologiciel des composants suivants :

- BIOS
- Lifecycle Controller
- iDRAC
- Pack de pilotes du système d'exploitation
- Diagnostics 32 bits
- CPLD de système
- Contrôleurs PERC
- Batteries
- Disques physiques
- Alimentation électrique
- Carte réseau
- Fibre Channel
- Fond de panier
- Enceinte
- Cartes SSD PCIe

Lorsque vous remplacez un composant matériel ou mettez à jour les versions micrologicielles, veillez à activer et exécuter l'option **CSIOR** (Collect System Inventory on Reboot - Collecter l'inventaire système au redémarrage) pour collecter l'inventaire du système lors du redémarrage. Après quelques minutes, ouvrez une session dans iDRAC7 et accédez à la page du **Inventaire du système** pour afficher les informations. Il se peut que les informations soient disponibles au bout de cinq minutes en fonction du matériel installé sur le serveur.

REMARQUE : L'option CSIOR est activée par défaut.

Cliquez sur **Exporter** pour exporter l'inventaire de matériel au format XML et l'enregistrer dans un emplacement de votre choix.

Affichage des informations des capteurs

Les capteurs suivant permettent de surveiller l'intégrité du système géré :

- **Batteries** : fournit des informations sur les batteries CMOS de la carte système et la carte ROMB (RAID On Motherboard) de stockage.

REMARQUE : Les paramètres de la batterie ROMB de stockage sont disponibles uniquement si le système dispose d'une care ROMB avec une batterie.

- **Ventilateur** (disponible uniquement pour les serveurs en rack et de type tour) : fournit des informations sur les ventilateurs du système (redondance de ventilateur et liste des ventilateurs qui indiquent la vitesse et les valeurs de seuil).
- **UC** : affiche l'intégrité et l'état des UC du système géré. Ce capteur rapporte également la limitation automatique des processeurs et les échecs prévisibles.
- **Mémoire** : affiche l'intégrité et l'état des barrettes de mémoire (DIMM) se trouvant sur le système géré.
- **Intrusion** : fournit des informations sur le châssis.
- **Blocs d'alimentation** (disponible uniquement sur les serveurs en rack et de type tour) : fournit des informations sur les blocs d'alimentation et l'état de redondance des blocs.

  REMARQUE : Si le système est doté d'un seul bloc d'alimentation, la redondance de bloc est **désactivée**.
- **Média flash amovible** : fournit des informations sur les modules SD internes : vFlash et module IDSDM (Internal Dual SD Module).
  - Lorsque la redondance IDSDM est activée, l'état du capteur IDSDM suivant est affiché : État de redondance IDSDM, IDSDM SD1, IDSDM SD2. Lorsqu'elle n'est pas activée, seul IDSDM SD1 est affiché.
  - Si la redondance IDSDM est désactivée initialement lorsque le système est mis sous tension ou après une réinitialisation d'iDRAC, l'état du capteur IDSDM SD1 est affiché uniquement après l'insertion d'une carte.
  - Si elle est activée avec deux cartes présentes dans IDSDM et que l'état d'une carte SD est *En ligne* alors que l'état de l'autre carte est *Hors ligne*, un redémarrage est nécessaire pour restaurer la redondance entre les deux cartes SD dans IDSDM. Une fois la redondance restaurée, l'état des deux cartes SD dans IDSDM est *En ligne*.
  - Au cours de l'opération de régénération pour restaurer la redondance entre les deux cartes SD présentes dans IDSDM, l'état IDSDM ne s'affiche pas, car les capteurs IDSDM sont hors tension.
  - Les journaux d'événements système (SEL) d'une carte protégée en écriture ou endommagée dans le module IDSDM ne sont pas répétés jusqu'à ce qu'ils soient effacés en remplaçant la carte SD par une carte SD inscriptible ou en bon état.
- **Température** : fournit des informations sur la température d'entrée et de sortie de la carte système (s'applique uniquement aux serveurs en rack et de type tour). Le capteur de température indique si son état correspond à la valeur de seuil d'avertissement et critique prédéfinie.
- **Tension** : indique l'état et les valeurs des capteurs de tension des divers composants du système.

Le tableau suivant explique comment afficher les informations des capteurs en utilisant l'interface Web d'iDRAC7 et l'interface RACADM. Pour plus d'informations sur les propriétés affichées dans l'interface Web, voir l'*aide en ligne d'iDRAC7* pour les pages correspondantes.

Tableau 10. Informations de capteurs en utilisant l'interface Web et l'interface RACADM

Affichage des informations des capteurs	Utilisation de l'interface Web	Utilisation de l'interface RACADM
Batteries	**Présentation générale → Matériel → Batteries**	Utilisez la commande **getsensorinfo**. Pour les blocs d'alimentations, vous pouvez également utiliser la commande **System.Power.Supply** avec la sous-commande **get**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC)

Affichage des informations des capteurs	Utilisation de l'interface Web	Utilisation de l'interface RACADM
		disponible à l'adresse **dell.com/support/manuals**.
Fan (Ventilateur)	**Présentation générale → Matériel → Ventilateurs**	
UC	**Présentation général → Matériel → Processeur**	
Mémoire	**Présentation → Matériel → Mémoire**	
Intrusion	**Présentation générale → Serveur → Intrusion**	
Blocs d'alimentation	**Présentation générale → Matériel → Blocs d'alimentation**	
Média flash amovible	**Présentation générale → Matériel → Média Flash amovible**	
Température	**Présentation générale → Serveur → Alimentation/Thermique → Températures**	
Tension	**Présentation générale → Serveur → Alimentation/Thermique → Tensions**	

Vérification de la conformité du système aux normes d'air frais

Le refroidissement à l'air frais utilise directement l'air extérieur pour refroidir les systèmes du centre de données. Les systèmes conformes aux normes d'air frais peuvent fonctionner au-dessus de leur plage de température ambiante de fonctionnement normale (températures jusqu'à 113 ° F (45 ° C)).

REMARQUE : La configuration d'air frais n'est pas prise en charge pour les disques SSD PCIe, cartes graphiques, barettes DIMM LR et UC 135W. Pour connaître les configurations d'air frais prises en charge pour le serveur, contactez Dell.

Pour vérifier la conformité du système aux normes d'air frais :

1. Dans l'interface Web iDRAC7, accédez à **Présentation → Serveur → Alimentation / Thermique → Températures**. La page **Températures** s'affiche.
2. Reportez-vous à la section **Air frais** qui indique si le serveur est conforme ou non aux normes d'air frais.

Affichage des données historiques de température

Vous pouvez surveiller le pourcentage de temps pendant lequel le système a fonctionné à une température ambiante supérieure au seuil de température normalement toléré. La lecture du capteur de température d'entrée du système est recueillie durant une certaine période pour surveiller la température. La collecte des données commence lorsque le système est mis sous tension après son expédition de l'usine. Les données sont collectées et affichées pendant tout le temps où le système est sous tension. Vous pouvez suivre et stocker la température d'entrée surveillée durant les sept dernières années.

REMARQUE : Vous pouvez suivre l'historique de la température d'entrée, même pour les systèmes qui ne sont pas conformes aux normes d'air frais.

Deux bandes de température sont suivies :

- Bande d'avertissement : temps pendant lequel un système a fonctionné au-dessus du seuil d'avertissement du capteur de température d'entrée. Le système peut fonctionner dans la bande d'avertissement durant 10 % du temps pendant 12 mois.
- Bande critique : temps pendant lequel un système a fonctionné au-dessus du seuil critique du capteur de température d'entrée. Le système peut fonctionner dans la bande critique durant 1 % du temps pendant 12 mois, ce qui incrémente également le temps dans la bande d'avertissement.

Les données collectées sont représentées sous forme graphique pour suivre les niveaux de 10 % et 1 %. Les données de température enregistrées ne peuvent être effacées qu'avant l'expédition de l'usine.

Un événement est généré si le système continue de fonctionner au-dessus du seuil de température normalement toléré durant une durée de fonctionnement spécifiée. Si la température moyenne sur la durée de fonctionnement spécifiée est supérieure ou égale au niveau d'avertissement (> = 0,8 %) ou au niveau critique (> = 0,8%), un événement est enregistré dans le journal Lifecycle et l'interruption SNMP correspondante est générée. Les événements sont les suivants :

- Événement d'avertissement lorsque la température d'entrée a été supérieure au seuil d'avertissement durant 8 % du temps ou plus au cours des 12 derniers mois.
- Événement critique lorsque la température d'entrée a été supérieure au seuil d'avertissement durant 10 % du temps ou plus au cours des 12 derniers mois.
- Événement d'avertissement lorsque la température d'entrée a été supérieure au seuil critique durant 0,8 % du temps ou plus au cours des 12 derniers mois.
- Événement critique lorsque la température d'entrée a été supérieure au seuil critique durant 1 % du temps ou plus au cours des 12 derniers mois.

Vous pouvez également configurer iDRAC pour générer des événements supplémentaires. Pour plus d'informations, consultez la section Définition d'événement de récurrence d'alerte.

Affichage des données historiques de température à l'aide de l'interface Web iDRAC7

Pour afficher les données historiques de température :

1. Dans l'interface Web iDRAC7, accédez à **Présentation** → **Serveur** → **Alimentation / Thermique** → **Températures**.
   La page **Températures** s'affiche.
2. Reportez-vous à la section **Données historiques de températures d'entrée de la carte système** qui fournit un affichage graphique des températures d'entrée stockées (valeurs moyennes et maximales) pour le dernier jour, les 30 derniers jours, et l'année passée.
   Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.

   REMARQUE : Après une réinitialisation d'iDRAC ou une mise à jour du micrologiciel iDRAC, certaines données de température peuvent ne pas être affichées dans le graphique.

Affichage des données historiques de température à l'aide de l'interface RACADM

Pour afficher les données historiques à l'aide de l'interface RACADM, utilisez la sous-commande **inlettemphistory**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC)*.

Inventaire et surveillance des périphériques de stockage

Vous pouvez surveiller à distance l'intégrité et afficher les périphériques de stockage CEM (Comprehensive Embedded Management) suivants dans le système géré en utilisant l'interface Web ou l'interface RACADM d'iDRAC7 :

- contrôleurs RAID contenant une batterie ;

- boîtiers contenant des modules EMM (Enclosure Management Modules), une alimentation électrique, un capteur de ventilateur et un capteur de température ;
- Disques physiques
- disques virtuels

Toutefois, WS-MAN affiche des informations pour la plupart des périphériques de stockage du système.

iDRAC7 inventorie et surveille les contrôleurs RAID PERC 8 Series qui contiennent H310, H710, H710P et H810. Les contrôleurs qui ne prennent pas en charge CEM (Comprehensive Embedded Management) sont les adaptateurs de bande internes (ITA) et les adaptateurs HBA SAS 6 Gbps.

Les derniers événements de stockage et la topologie des périphériques de stockage sont également affichés.

Des alertes et des interruptions SNMP sont générées pour les événements de stockage. Les événements sont consignés dans le journal Lifecycle.

Pour les informations conceptuelles, voir le *Guide d'utilisation d'OpenManage Storage Management* disponible à l'adresse **dell.com/support/manuals**.

Surveillance des périphériques de stockage avec l'interface Web

Pour afficher les informations des périphériques de stockage en utilisant l'interface Web :

- Accédez à **Présentation générale** → **Stockage** → **Résumé** pour afficher le résumé des composants de stockage et les derniers événements consignés. Cette page est actualisée automatiquement toutes les 30 secondes.
- Accédez à **Présentation générale** → **Stockage** → **Topologie** pour afficher la vue de relation physique hiérarchique des principaux composants de stockage.
- Accédez à **Présentation générale** → **Stockage** → **Disques physiques** pour afficher les informations des disques physiques. La page **Disques physiques** s'affiche.
- Accédez à **Présentation générale** → **Stockage** → **Disques virtuels** pour afficher des informations sur les disques virtuels. La page **Disques virtuels** s'affiche.
- Accédez à **Présentation générale** → **Stockage** → **Contrôleurs** pour afficher les informations des contrôleurs RAID. La page **Contrôleurs** s'affiche.
- Accédez à **Présentation générale** → **Stockage** → **Enceintes** pour afficher les informations des enceintes. La page **Enceintes** s'affiche.

Vous pouvez également utiliser des filtres pour afficher les informations relatives à des périphériques spécifiques.

Pour plus d'informations sur les propriétés affichées et l'utilisation des options, voir l'*Aide en ligne d'iDRAC7*.

Surveillance d'un périphérique de stockage en utilisant l'interface RACADM

Pour afficher les informations d'un périphérique de stockage, utilisez la commande **raid**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Inventaire et surveillance des périphériques réseau

Vos pouvez surveiller à distance l'intégrité et afficher l'inventaire des périphériques réseau suivant dans le système géré :

- Cartes d'interface réseau (NIC)
- Adaptateurs réseau de convergence (CNA)
- Cartes LOM (LAN On Motherboard)
- Cartes NCD (Network Daughter Card)

- Cartes mezzanines (uniquement pour les serveurs lames)

Pour chaque périphérique, vous pouvez afficher les informations suivantes sur les ports et les partitions prises en charge.

- État de la liaison
- Propriétés
- Paramètres et capacités
- Statistiques de réception et de transmission

Liens connexes

Activation ou désactivation de l'optimisation d'identité d'E/S

Surveillance des périphériques réseau en utilisant l'interface Web

Pour afficher les informations des périphériques réseau en utilisant l'interface Web, accédez à **Présentation générale → Matériel → Périphériques réseau**. La page **Périphériques réseau** s'affiche. Pour plus d'informations sur les propriétés affichées, voir l'*Aide en ligne d'iDRAC7*.

REMARQUE : Si l'**État des pilotes SE** signale qu'ils sont opérationnels, il indique l'état de pilotes du système d'exploitation ou d'UEFI

Surveillance des périphériques réseau en utilisant l'interface RACADM

Pour afficher les informations des périphériques réseau, utilisez les commandes **hwinventory** et **nicstatistics**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

D'autres propriétés peuvent être affichées lors de l'utilisation de l'interface RACADM ou de WS-MAN en plus des propriétés affichées dans l'interface Web iDRAC7.

Activation ou désactivation de l'optimisation d'identité d'E/S

Normalement, après le démarrage du système, les périphériques sont configurés, puis les périphériques sont initialisés après un redémarrage. Vous pouvez configurer la fonction Optimisation de l'identité d'E/S pour effectuer un démarrage optimal. Si la fonction est activée, elle définit les attributs d'adresse virtuelle, d'initiateur et de cible de stockage après la réinitialisation du périphérique et avant son initialisation, éliminant ainsi le besoin d'un deuxième redémarrage du BIOS. L'opération de configuration et de démarrage du périphérique survient lors du démarrage unique du système et est optimisée pour les performances du temps d'amorçage.

Avant d'activer l'optimisation de l'identité d'E/S, assurez-vous que :

- Vous détenez des privilèges de connexion, de configuration et de contrôle du système.
- Le BIOS, l'iDRAC et les cartes réseau sont mis à jour à la version la plus récente du micrologiciel. Pour plus d'informations sur les versions prises en charge, voir Version du BIOS prise en charge pour l'optimisation de l'identité d'E/S et Version du micrologiciel de carte réseau prise en charge pour l'optimisation de l'identité d'E/S.

Après l'activation de la fonction d'optimisation d'identité d'E/S, exportez le fichier de configuration XML d'iDRAC, modifiez les attributs d'identité d'E/S requis dans le fichier de configuration XML et réimportez le fichier sur iDRAC.

Pour obtenir la liste des attributs d'optimisation d'identité d'E/S que vous pouvez modifier dans le fichier de configuration XML, voir le document *Profil de carte réseau* disponible sur **delltechcenter.com/idrac**.

REMARQUE : Ne modifiez pas les attributs autres que ceux d'optimisation d'identité d'E/S.

Cartes prises en charge pour l'optimisation d'identité d'E/S

Le tableau suivant indique les cartes qui prennent en charge la fonction d'optimisation d'identité d'E/S.

Fabricant	Type
Broadcom	• 5720 PCIe 1 Go • 5719 PCIe 1 Go • 57810 PCIe 10 Go • 57810 PCIe 10 Go • 57810 bNDC 10 Go • 57800 rNDC 10 Go + 1 Go • 57800 rNDC 10 Go + 1 Go • 57840 rNDC 10 Go • 57840 bNDC 10 Go • 5720 rNDC 1 Go • 5719 Mezz 1 Go • 57810 Mezz 10 Go
Intel	• x540 PCIe 10 Go • x520 PCIe 10 Go • i350 PCIe 1 Go • i350 PCIe 1 Go • x540 + i350 rNDC 10 Go + 1 Go • i350 rNDC 1 Go • x520 bNDC 10 Go • i350 Mezz 1 Go • x520 + i350 rNDC 10 Go + 1 Go
QLogic	• QLE8262 PCIe 10 Go • QME8262 Mezz 10 Go • QMD8262 bNDC 10 Go

REMARQUE : L'optimisation d'identité d'E/S n'est pas prise en charge sur les cartes suivantes :

- Cartes Emulex
- Cartes Fibre Channel
- Intel x520 Mezz 10 Go

Version du BIOS prise en charge pour l'optimisation d'identité E/S

Le tableau suivant répertorie la version BIOS minimale prise en charge sur les serveurs PowerEdge de 12e génération.

Serveur Dell PowerEdge de 12e génération	Versions BIOS minimales prises en charge
R720, R720xd, R620, T620 et M620	2.1.0
R820	2.0.15
R520, R320, R420, T420, T320, M520 et M420	2.0.19

Serveur Dell PowerEdge de 12e génération	Versions BIOS minimales prises en charge
M820	1.7.0

Versions du micrologiciel de carte réseau prises en charge pour l'optimisation d'identité d'E/S

Le tableau suivant indique les versions du micrologiciel de la carte réseau pour la fonctionnalité d'optimisation d'identité d'E/S.

Fabricant	Version du micrologiciel de la carte d'interface réseau prise en charge
Cartes Broadcom	7.8.x
Cartes Intel	15.0.x
QLogic 82xx (CNA)	1.13.x/6.0.0.x

Activation ou désactivation de l'optimisation d'identité d'E/S via l'interface Web

Pour activer ou désactiver l'optimisation d'identité d'E/S :

1. Dans l'interface Web iDRAC, accédez à **Présentation générale** → **Matériel** → **Périphériques réseau**.
   La page **Résumé des périphériques réseau** s'affiche.
2. Dans la section **Paramètres d'identité d'E/S**, sélectionnez l'option **Optimisation d'identité d'E/S** pour que cette fonction soit opérationnelle. Pour désactiver, décochez cette option.
3. Cliquez sur **Appliquer** pour appliquer le paramètre.

Activation ou désactivation de l'optimisation d'identité d'E/S à l'aide de RACADM

Pour activer l'optimisation d'identité d'E/S, utilisez la commande :

```
racadm set idrac.ioidopt.IOIDOptEnable 1
```

Après l'activation de cette fonction, vous devez redémarrer le système pour que les paramètres soient pris en compte.

Pour désactiver l'optimisation d'identité d'E/S, utilisez la commande :

```
racadm set idrac.ioidopt.IOIDOptEnable 0
```

Pour afficher le réglage de l'optimisation d'identité d'E/S, utilisez la commande :

```
racadm get iDRAC.IOIDOpt
```

Inventaire et surveillance des périphériques HBA FC

Vous pouvez surveiller l'intégrité à distance et afficher l'inventaire des adaptateurs de bus hôte (HBA) Fibre Channel dans le système géré. Les HBA FC Emulex et QLogic (sauf FC8) sont pris en charge. Vous pouvez afficher les informations suivantes sur les ports de chaque périphérique HBA FC :

- Informations et état des liaisons
- Propriétés du port
- Statistiques de réception et de transmission

Surveillance des périphériques HBA FC à l'aide de l'interface Web

Pour afficher les informations des périphériques HBA FC à l'aide de l'interface Web, allez sous **Présentation** → **Matériel** → **Fibre Channel**. La page FC s'affiche. Pour en savoir plus sur les propriétés affichées, voir l'*aide en ligne iDRAC7*.

Le nom de la page affiche également le numéro du logement comportant le périphérique HBA FC disponible et le type de périphérique qu'il contient.

Surveillance des périphériques HBA FC à l'aide de RACADM

Pour afficher les informations de périphérique HBA FC à l'aide de racadm, utilisez la sous-commande **hwinventory**. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Visualisation des connexions de structure des cartes mezzanines FlexAddress

Dans les serveurs lames, FlexAddress permet d'utiliser des noms mondiaux et des adresses MAC (WWN/MAC) persistants assignés par le châssis pour chaque connexion de port de serveur géré.

Vous pouvez afficher les informations suivantes pour chaque port de carte Ethernet intégrée et mezzanine en option :

- Structures auxquelles les cartes sont connectées.
- Type de structure.
- Adresses MAC affectées par le serveur, par le châssis ou à distance.

Pour afficher les informations Flex Address dans iDRAC7, configurez et activez la fonction Flex Address dans CMC (Chassis Management Controller). Pour plus d'informations, voir le *Dell Chassis Management Controller User Guide* (Guide d'utilisation Dell Chassis Management Controller) disponible sur le site **dell.com/support/manuals**. Les sessions de console virtuelle ou Média Virtuel existantes prennent fin si le paramètre FlexAddress est activé ou désactivé.

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

La fonction FlexAddress remplace les adresses MAC affectées par le serveur par des adresses MAC affectées par le châssis et elle est mise en oeuvre pour iDRAC7 avec les LOM de lame, les cartes mezzanines et les module d'E/S. La fonction iDRAC7 FlexAddress prend en charge la conservation des adresses MAC de logement pour les iDRAC7 dans un châssis. L'adresse MAC affectée par le châssis est stockée dans la mémoire non volatile CMC et elle est envoyée à iDRAC7 pendant son démarrage ou lorsque CMC FlexAddress est activé.

Si CMC permet d'utiliser des adresses MAC affectées par le châssis, iDRAC7 affiche l'**adresse MAC** dans les pages suivantes :

- **Présentation → Serveur → Propriétés Détails → Informations iDRAC** .
- **Présentation → Serveur → Propriétés WWN/MAC**.
- **Présentation générale → Paramètres iDRAC → Propriétés Informations iDRAC → Paramètres réseau actuels**.
- **Présentation → Paramètres iDRAC → Réseau Réseau → Paramètres réseau**.

PRÉCAUTION : Lorsque FlexAddress est activé, si vous passez d'une adresse MAC affectée par le serveur à une adresse MAC attribuée par le châssis et vice–versa, l'adresse IP iDRAC7 change également.

Affichage ou fin des sessions iDRAC7

Vous pouvez afficher le nombre d'utilisateurs connectés à iDRAC7 et mettre fin aux sessions utilisateur.

Fin des sessions iDRAC7 en utilisant l'interface Web

Les utilisateurs ne disposant pas de privilèges d'administrateur doivent avoir le privilège de configuration iDRAC7 pour pouvoir mettre à fins aux sessions iDRAC7 en utilisant l'interface Web d'iDRAC7.

Pour afficher les sessions iDRAC7 et y mettre fin :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Sessions**.
   La page **Sessions** affiche l'ID de session, le nom d'utilisateur, l'adresse IP et le type de session. Pour plus d'informations sur ces propriétés, voir l'*aide en ligne d'iDRAC7*.
2. Pour mettre fin à la session, dans la colonne **Annuler**, cliquez sur l'icône de corbeille pour la session.

Fin des sessions iDRAC7 en utilisant l'interface RACADM

Vous devez disposer des privilèges d'administrateur pour pouvoir mettre fin aux sessions iDRAC7 en utilisant l'interface RACADM.

Pour afficher les sessions utilisateur en cours, utilisez la commande **getssninfo**.

Pour mettre fin à une session utilisateur, utilisez la commande **closessn**.

Pour plus d'informations sur ces commandes, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible à l'adresse **dell.com/support/manuals**.

6

Configuration de la communication iDRAC7

Vous pouvez communiquer avec iDRAC7 en utilisant les modes suivants :

- Interface Web iDRAC7
- Connexion série en utilisant un câble DB9 (RAC série ou IPMI sériel). S'applique aux serveurs en rack et de type tour uniquement.
- IPMI série sur LAN
- IPMI sur le LAN
- Interface RACADM distante
- Interface RACADM locale
- Services à distance

Pour la présentation des protocoles pris en charge, des commandes prises en charge et les conditions requises, voir le tableau suivant.

Tableau 11. Modes de communication — Résumé

Mode de communication	Protocole pris en charge	Commandes prises en charge	Conditions requises
Interface Web iDRAC7	Protocole Internet (https)	S/O	Web Server
Série en utilisant un câble Null modem DB9	Protocole série	RACADM SMCLP IPMI	Partie du micrologiciel d'iDRAC7 RAC Série ou IPMI Série est activé
IPMI série sur LAN	Protocole IPMB (Intelligent Platform Management Bus) SSH Telnet	IPMI	IPMITool est installé et IPMI série sur le LAN est activé.
IPMI sur le LAN	Protocole IPMB (Intelligent Platform Management Bus)	IPMI	IPMITool est installé et les paramètres IPMI sont activés.
SMCLP	SSH Telnet	SMCLP	SSH ou Telnet sur iDRAC7 est activé.
Interface RACADM distante	HTTPS	Interface RACADM distante	L'interface distance RACADM est installée et activée.
Micrologiciel RACADM	SSH Telnet	Micrologiciel RACADM	Le micrologiciel RACADM est installé et activé.
Interface RACADM locale	IPMI	Interface RACADM locale	L'interface RACADM locale est installée.
Services distants [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM est installé (Windows) ou

Mode de communication	Protocole pris en charge	Commandes prises en charge	Conditions requises
			OpenWSMAN est installé (Linux).

[1] Pour plus d'informations, voir le *Lifecycle Controller Remote Services User's Guide* (Guide d'utilisation des services à distance Lifecycle Controller) disponible à l'adresse **dell.com/support/manuals**.

Liens connexes

Communication avec iDRAC7 via une connexion série en utilisant un câble DB9
Permutation entre RAC Série et la console série à l'aide d'un câble DB9
Communication avec iDRAC7 en utilisant SOL IPMI
Communication avec iDRAC7 en utilisant IPMI sur LAN
Activation ou désactivation de l'interface distance RACADM
Désactivation de l'interface locale RACADM
Activation d'IPMI sur un système géré
Configuration de Linux pour la console série pendant le démarrage
Schémas cryptographiques SSH pris en charge

Communication avec iDRAC7 via une connexion série en utilisant un câble DB9

Vous pouvez utiliser les modes de communication suivants pour exécuter les tâches de gestion de systèmes via une connexion série aux serveurs racks ou de type tour :

- RAC série
- IPMI série — Mode de base de connexion directe et mode terminal de connexion directe

REMARQUE : Dans le cas de serveurs lames, la connexion série est établie via le châssis. Pour plus d'informations, voir le *Chassis Management Controller User's Guide* (Guide d'utilisation du Chassis Management Controller) disponible sur l'adresse **dell.com/support/manuals**.

Pour établir la connexion série :

1. Configurez le BIOS pour activer la connexion série :
2. Connectez le câble Null Modem DB9 du port série de la station de gestion au connecteur série externe du système géré.
3. Vérifiez que le logiciel d'émulation de terminal de la station de gestion est configuré pour la connexion série en utilisant l'un des éléments suivants :
   - Linux Minicom dans un Xterm
   - HyperTerminal Private Edition (version 6.3) de Hilgraeve

   Selon le point en cours du processus de démarrage du système géré, vous pouvez voir l'écran du POST ou celui du système d'exploitation. Ceci dépend de la configuration : SAC pour Windows et des écrans du mode texte Linux pour Linux.
4. Activez la connexion RAC série ou IPMI série dans iDRAC7.

Liens connexes

Configuration du BIOS pour une connexion série
Activation d'une connexion série RAC
Activation des modes de base et terminal de connexion série IPMI

Configuration du BIOS pour une connexion série

Pour configurer le BIOS pour une connexion série :

REMARQUE : Ces informations s'appliquent uniquement à iDRAC7 sur un serveur en rack ou de type tour.

1. Activez ou redémarrez le système géré.
2. Appuyez sur <F2>.
3. Accédez à **System BIOS Settings** → **Serial Communication** (Paramètres du BIOS du système, Communication série).
4. Sélectionnez **External Serial Connector** to **Remote Access device** (Connecteur série externe vers périphérique d'accès à distance).
5. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
6. Appuyez sur <Échap> pour quitter la **configuration du système**.

Activation d'une connexion série RAC

Après avoir configuré la connexion série dans le BIOS, activez RAC série dans iDRAC7.

REMARQUE : Ceci s'applique uniquement à iDRAC7 sur les serveurs en rack et de type tour.

Activation de la connexion RAC série en utilisant l'interface Web

Pour activer la connexion RAC série :

1. Dans l'interface Web d'iDRAC7, accédez à **Overview** → **iDRAC Settings** → **Network** → **Serial** (Présentation générale, Paramètres iDRAC, Réseau, Série)

   La page **Serial** (Série) s'affiche.
2. Sous **RAC série**, sélectionnez **Activé** et spécifiez les valeurs des attributs.
3. Cliquez sur **Apply** (Appliquer).

   Les paramètres série IPMI sont définis.

Activation de la connexion RAC série à l'aide de l'interface RACADM

Pour activer la connexion série RAC avec RACADM, utilisez l'une des méthodes suivantes :

- Utilisez les objets du groupe **cfgSerial** avec la commande **config**.
- Utilisez l'objet du groupe **iDRAC.Serial** avec la commande **set**.

Activation des modes de base et terminal de connexion série IPMI

Pour activer le routage série IPMI du BIOS vers iDRAC7, configurez IPMI série dans les modes suivants dans iDRAC7 :

REMARQUE : Ceci s'applique uniquement à iDRAC7 sur les serveurs en rack et de type tour.

- Mode de base IPMI — Prend en charge une interface binaire pour l'accès au programme, telle que IPMI shell (ipmish) qui est inclus dans BMU (Baseboard Management Utility). Par exemple, pour imprimer le journal des événements système en utilisant ipmish via le mode de base IPMI, exécutez la commande suivante :

  ```
  ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
  ```
- Mode terminal IPMI— Prend en charge les commandes ASCII envoyées depuis un terminal série. Ce mode prend en charge un nombre limité de commandes (y compris le contrôle de l'alimentation) et de commandes IPMI brutes tapées sous forme de caractères hexadécimaux. Il permet d'afficher les séquences de démarrage du système d'exploitation jusqu'au BIOS lorsque vous vous ouvrez une session dans iDRAC7 via SSH ou Telnet.

Liens connexes

Configuration du BIOS pour une connexion série
Autres paramètres pour le mode Terminal série IPMI

Activation d'une connexion série en utilisant l'interface Web

Veillez à désactiver l'interface RAC série pour activer IPMI série.

Pour définir les paramètres IPMI série :

1. Dans l'interface Web d'iDRAC7, accédez à **Overview** → **iDRAC Settings** → **Network** → **Serial** (Présentation générale, Parmètres iDRAC, Réseau, Série).
2. Sous **IPMI sériel**, spécifiez les valeurs des attributs. Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC7*.
3. Cliquez sur **Apply** (Appliquer).

Activation du mode IPMI de connexion série en utilisant l'interface RACADM

Pour configurer le mode IPMI, désactivez l'interface série RAC, puis activez le mode IPMI à l'aide d'une des commandes suivantes :

- Avec la commande **config** :

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

  racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode < 0  or  1>
  ```

  , où *0* indique le mode Terminal et *1*, le mode de base.
- Avec la commande **set** :

  ```
  racadm set iDRAC.Serial.Enable 0

  racadm set iDRAC.IPMISerial.ConnectionMode < 0  or  1>
  ```

  , où *0* indique le mode Terminal et *1*, le mode de base.

Activation des paramètres série IPMI de connexion série en utilisant l'interface RACADM

Pour configurer les paramètres série IPMI, utilisez la commande **set** ou **config** :

1. Remplacez le mode de connexion série IPMI par le mode série approprié en utilisant la commande suivante :
   - Avec la commande **config** : `racadm config -g cfgSerial -o cfgSerialConsoleEnable 0`
   - Avec la commande **set** : `racadm set iDRAC.Serial.Enable 0`
2. Configurez le débit en bauds des communications IPMI série :
   - Avec la commande **config** : `racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <débit_en_bauds>`
   - Avec la commande **set** : `racadm set iDRAC.IPMISerial.BaudRate <débit_en_bauds>`

   où `<débit_en_bauds>` est égal à 9 600, 19 200, 57 600 ou 115 200 b/s.
3. Activez le contrôle du débit matériel des communications IPMI série :
   - Avec la commande **config** : `racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1`
   - Avec la commande **set** : `racadm set iDRAC.IPMISerial.FlowControl 1`

4. Configurez le niveau de privilège minimal de canal des communications IPMI série :

   – Avec la commande **config** : `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <niveau>`
   – Avec la commande **set** : `racadm set iDRAC.IPMISerial.ChanPrivLimit <niveau>`

   où `<niveau>` correspond à `2` (Utilisateur), `3` (Opérateur), ou `4` (Administrateur).

5. Vérifiez que le connecteur MUX (connecteur série externe) est correctement défini sur le périphérique d'accès à distance dans le programme de configuration du BIOS pour configurer le BIOS pour la connexion série.

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

Autres paramètres pour le mode Terminal série IPMI

Cette section fournit des informations sur les paramètres de configuration du mode Terminal série IPMI.

Définition d'autres paramètres pour le mode Terminal série IPMI en utilisant l'interface Web

Pour définir les paramètres du mode Terminal série :

1. Dans l'interface Web d'iDRAC7, accédez à Overview**iDRAC SettingsNetworkSerial** (Présentation générale, Parmètres iDRAC, Réseau, Série).

   La page **Serial** (Série) s'affiche.

2. Activez l'option IPMI serial (Série IMPI).
3. Cliquez sur **Paramètres du mode terminal** .

   La page **Paramètres du mode terminal** s'affiche.

4. Définissez les valeur suivantes :

   – Modification de ligne
   – Contrôle de la suppression
   – Contrôle d'écho
   – Contrôle de l'établissement de liaisons
   – Nouvelle séquence linéaire
   – Saisie de nouvelles séquences linéaires

   Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC7*.

5. Cliquez sur **Apply** (Appliquer).

   Les paramètres du mode Terminal sont définis.

6. Vérifiez que le connecteur MUX (connecteur série externe) est configuré correctement sur le périphérique d'accès à distance dans le programme de configuration du BIOS pour configurer le BIOS pour la connexion série.

Définition de paramètres supplémentaires pour le mode Terminal IPMI série en utilisant l'interface RACADM

Pour configurer les paramètres du mode Terminal, exécutez la commande `racadm config cfgIpmiSerial`

Permutation entre RAC Série et la console série à l'aide d'un câble DB9

iDRAC7 prend en charge les séquences de touches d'échappement qui permettent de permuter entre la communication avec l'interface RAC Série et la console série sur les serveurs en rack ou de type tour.

Passage de la console série à RAC Série

Pour passer au mode de communication RAC Série lorsque vous utilisez le mode Console série, utilisez la séquence de touches suivante :

```
<Échap> + <Maj> <9>
```

La séquence de touches vous dirige vers l'invite « Ouverture de session sur iDRAC » (si le RAC est défini sur le mode « RAC série ») ou active le mode « Connexion série » où des commandes de terminal peuvent être émises (si le iDRAC est défini sur « Connexion directe IPMI série en mode terminal »).

Passage du mode RAC Série au mode Console série

Pour passer au mode Console série lorsque vous utilisez le mode de communication d'interface série RAC, utilisez la séquence de touches suivante :

```
<Échap> + <Maj> <q>
```

Lorsque vous utilisez le mode terminal, pour passer en mode Console série, utilisez :

```
<Échap> + <Maj> <q>
```

Pour revenir au mode Terminal, lorsque vous êtes connecté en mode Console série :

```
<Échap> + <Maj> <9>
```

Communication avec iDRAC7 en utilisant SOL IPMI

SOL (Serial Over LAN) IPMI permet aux données série de la console texte d'un système géré d'être redirigées sur un réseau de gestion Ethernet hors bande partagé ou dédié d'iDRAC7. Avec SOL, vous pouvez :

- accéder à distance aux systèmes d'exploitation sans expiration de délai d'attente ;
- diagnostiquer des systèmes hôtes sur Emergency Management Services (EMS) ou Special Administrator Console (SAC) pour Windows ou dans un environnement Linux ;
- afficher l'avancement d'un serveur au cours du POST et reconfigurer le programme de configuration du BIOS.

Pour définir le mode de communication SOL :

1. Configurez le BIOS pour une connexion série.
2. Configurez iDRAC7 pour utiliser SOL.
3. Activez un protocole pris en charge (SSH, Telnet, IPMItool).

Liens connexes

Configuration du BIOS pour une connexion série
Configuration d'iDRAC7 pour utiliser SOL
Activation du protocole pris en charge

Configuration du BIOS pour une connexion série

Pour configurer le BIOS pour une connexion série :

REMARQUE : Ces informations s'appliquent uniquement à iDRAC sur des serveurs en rack et de type tour.

1. Mettez le système sous tension ou redémarrez-le.
2. Appuyez sur <F2>.
3. Accédez à **Paramètres BIOS du système** → **Communication série**.

4. Définissez les valeurs suivantes :
   - Communication série — Activé avec redirection de console
   - Adresse de port série — COM2.

     REMARQUE : Vous pouvez définir le champ **Communications série** sur **Activé avec la redirection série via com1** si le **périphérique série 2** dans le champ **Adresse du port série** contient également com1.
   - Connecteur série externe -- Périphérique série 2
   - Débit Failsafe — 115 200
   - Type de terminal distant — VT100/VT220
   - Redirection après démarrage — Activé
5. Cliquez sur **Suivant**, puis sur **Terminer**.
6. Cliquez sur **Oui** pour enregistrer les modifications.
7. Appuyez sur <Échap> pour quitter la **configuration du système**.

Configuration d'iDRAC7 pour utiliser SOL

Vous pouvez définir les paramètres SOL dans iDRAC7 en utilisant l'interface Web, l'interface RACADM ou l'utilitaire de configuration d'iDRAC.

Configuration d'iDRAC7 pour utiliser SOL à l'aide de l'interface Web iDRAC7

Pour configurer IPMI sur le LAN (SOL) :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → Communication série sur le LAN**.

   L'écran **Communications série sur le LAN** apparaît.
2. Activez SOL, définissez les valeurs et cliquez sur **Appliquer**.

   Les paramètres SOL IPMI sont définis.
3. Pour définir la fréquence d'accumulation de caractères et le seuil d'envoi de caractères, sélectionnez **Paramètres avancés.**

   L'écran **Paramètres avancés Communication série sur LAN** s'affiche.
4. Définissez les valeurs des attributs et cliquez sur **Appliquer**.

   Les paramètres avancés SOL IPMI sont définis. Ces valeurs améliorent les performances.

   Pour plus d'informations sur les options, voir l'*Aide en ligne iDRAC7*.

Configuration d'iDRAC7 pour utiliser SOL en utilisant l'interface RACADM

Pour configurer IPMI sur le LAN (SOL) :

1. Activer IPMI sur le LAN
   - Avec la commande **config** : `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`
   - Avec la commande **set** : `racadm set iDRAC.IPMISol.Enable 1`
2. Mettez à jour le niveau de privilège minimal d'IPMI SOL :
   - Avec la commande **config** : `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <niveau>`
   - Avec la commande **set** : `racadm set iDRAC.IPMISol.MinPrivilege 1`

   où `<niveaul>` est 2 (Utilisateur), 3 (Opérateur), 4 (Administrateur).

   REMARQUE : Le niveau de privilège minimum IPMI SOL détermine le privilège minimum pour activer IPMI SOL. Pour plus d'informations, voir la spécification IPMI 2.0.
3. Mettez à jour le débit en bauds d'IPMI SOL :
   - Avec la commande **config** : `racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <débit_en_bauds>`
   - Avec la commande **set** : `racadm set iDRAC.IPMISol.BaudRate <débit_en_bauds>`

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

   REMARQUE : Pour rediriger la console série sur LAN, assurez-vous que le débit en bauds de SOL est identique à celui du système géré.
4. Activez SOL pour chaque utilisateur :
   - Avec la commande **config** : `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2`
   - Avec la commande **set** : `racadm set iDRAC.Users.<id>.SolEnable 2`

   où `<id>` est la référence unique de l'utilisateur.

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

Activation du protocole pris en charge

Les protocoles pris en charge sont IPMI, SSH et Telnet.

Activation d'un protocole compatible en utilisant l'interface Web

Pour activer SSH ou Telnet, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau** → **Services** et sélectionnez **Activé** pour SSH ou Telnet.

Pour activer IPMI, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau** et sélectionnez **Activer IPMI sur le LAN**. Vérifiez que la valeur **Clé de cryptage** correspond à des zéros ou appuyez sur la touche Retour arrière pour remplacer la valeur par des caractères NULL.

Activation d'un protocole compatible en utilisant l'interface RACADM

Pour activer SSH ou Telnet, exécutez la commande suivante :

- Telnet :
  - Avec la commande **config** : `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
  - Avec la commande **set** : `racadm set iDRAC.Telnet.Enable 1`
- SSH :
  - Avec la commande **config** : `racadm config -g cfgSerial -o cfgSerialSshEnable 1`
  - Avec la commande **set** : `racadm set iDRAC.SSH.Enable 1`

  Pour changer le port SSH :
  - Avec la commande **config** :`racadm config -g cfgRacTuning -o cfgRacTuneSshPort <numéro_de_port>`
  - Avec la commande **set** :`racadm set iDRAC.SSH.Port <numéro_de_port>`

Vous pouvez utiliser les outils suivants, entre autres :

- IPMItool pour utilisation du protocole IPMI
- Putty/OpenSSH pour utilisation du protocole SSH ou Telnet

Liens connexes

SOL en utilisant le protocole IPMI
SOL en utilisant le protocole SSH ou Telnet

SOL en utilisant le protocole IPMI

IPMItool <-->Connexion LAN/WAN <--> iDRAC7

L'utilitaire SOL basé sur IPMI et IPMItool utilise RMCP+ fourni en utilisant des datagrammes UDP vers le port 623. RMCP + améliore l'authentification, la vérification de l'intégrité des données et le cryptage et permet de transporter plusieurs types de charges utiles en utilisant IPMI 2.0. Pour plus d'informations voir **http://ipmitool.sourceforge.net/manpage.html**.

RMCP+ utilise une clé de cryptage sous la forme d'une chaîne hexadécimale de 40 caractères (caractères 0-9, a-f et A-F) pour l'authentification. La valeur par défaut est une chaîne de 40 zéros.

Une connexion RMCP+ à iDRAC7 doit être cryptée en utilisant la clé de cryptage (Key Generator (KG)Key). Vous pouvez définir la clé de cryptage en utilisant l'interface Web iDRAC7 ou l'utilitaire de configuration iDRAC.

Pour démarrer une session SOL en utilisant IPMItool depuis une station de gestion :

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente SOL par défaut dans **Présentation générale → Paramètres iDRAC → Réseau → Services**.

1. Installez IPMITool depuis le DVD *Dell Systems Management Tools and Documentation*.

   Pour les instructions d'installation, voir le *Guide d'installation rapide du logiciel*.
2. Depuis l'invite de commande (Windows ou Linux), exécutez la commande pour démarrer SOL depuis DRAC7 : `ipmitool -H <adresse ip iDRAC7> -I lanplus -U <nom de connexion> -P <mot de passe de connexion> sol activate`

   Elle permet de connecter la station de gestion au port série du système géré.
3. Pour quitter une session SOL depuis IPMItool, appuyez successivement sur <~> et sur <.>. La session SOL se ferme.

   REMARQUE : Si une session SOL ne se termine pas, réinitialisez iDRAC7 et attendez la fin du redémarrage qui peut prendre jusqu'à deux minutes.

SOL en utilisant le protocole SSH ou Telnet

SSH (Secure Shell) et Telnet sont des protocoles de réseau qui permettent d'exécuter des communications de ligne de commande avec iDRAC7. Vous pouvez analyser les commandes de l'interface distante RACADM et SMCLP via l'une ou l'autre de ces interfaces.

SSH est plus sécurisé que Telnet. iDRAC7 prend uniquement en charge la version SSH 2, avec l'authentification par mot de passe, qui est activée par défaut. iDRAC7 prend en charge jusqu'à deux sessions SSH et deux sessions Telnet simultanément. Il est recommandé d'utiliser SSH, car Telnet n'est pas un protocole sécurisé. Vous devez utiliser Telnet uniquement si vous ne pouvez pas installer un client SSH ou que l'infrastructure réseau est sécurisée.

Utilisez des programmes Open Source, tels que PuTTY ou OpenSSH, qui prennent en charge les protocoles de réseau SSH et Telnet sur une station de gestion pour vous connecter à iDRAC7.

REMARQUE : Exécutez `OpenSSH` depuis un émulateur de terminal VT100 ou ANSI sur Windows. L'exécution de `OpenSSH` depuis l'invite de commande Windows ne permet pas de disposer de la fonctionnalité complète (à savoir que certaines touches ne répondent pas et qu'aucun graphique ne s'affiche).

Avant d'utiliser SSH ou Telnet pour communiquer avec iDRAC7, veillez à :

1. configurer le BIOS pour activer la console série ;.
2. configurer SOL dans iDRAC7 ;
3. Activer SSH ou Telnet en utilisant l'interface Web iDRAC7 ou l'interface RACADM.

   Telnet (port 23)/ client SSH (port 22) <--> Connexion WAN <--> iDRAC7

   SOL basé sur IPMI, qui utilise le protocole SSH ou Telnet, évite d'avoir à utiliser un utilitaire supplémentaire, car la conversion série-réseau s'effectue dans iDRAC7. La console SSH ou Telnet que vous utilisez doit pouvoir interpréter les données envoyées par le port série du système géré et y répondre. Le port série se connecte généralement à un environnement qui émule un terminal ANSI ou VT100/VT220. La console série est redirigée automatiquement vers la console SSH ou Telnet.

Liens connexes

Utilisation de SOL depuis Putty On Windows
Utilisation de SOL depuis OpenSSH ou Telnet sur Linux

Utilisation de SOL depuis Putty On Windows

Pour démarrer SOL IPMI depuis PuTTY sur une station de gestion Windows :

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente SSH ou Telnet par défaut dans **Présentation générale → Paramètres iDRAC → Réseau → Services**.

1. Exécutez la commande suivante pour vous connecter à iDRAC7: `putty.exe [-ssh | -telnet] <nom de connexion>@<adresse IP iDRAC7> <numéro de port>`

   REMARQUE : Le numéro de port est facultatif. Il est nécessaire uniquement lorsque le numéro de port est réaffecté.

2. Exécutez la commande `console com2` ou `connect` pour démarrer SOL et le système géré.

   Une session SOL depuis la station de gestion vers le système géré, utilisant le protocole SSH ou Telnet, est ouverte. Pour accéder à la console de ligne de commande iDRAC7, suivez la séquence de touche ÉCHAP. Comportement de connexion de Putty et SOL :

   – Lors de l'accès au système géré via putty au cours du POST, si les touches de fonction et l'option de pavé de touches dans putty sont :

     * VT100+ — F2 passe, mais pas F12
     * ESC[n~ — F12 passe, mais pas F2

   – Dans Windows, l'ouverture de la console EMS (Emergency Management System) immédiatement après le redémarrage de l'hôte, peut endommager le terminal SAC (Special Admin Console). Quittez la session SOL, fermez le terminal, ouvrez un autre terminal et démarrez la session SOL en utilisant la même commande.

Liens connexes

Déconnexion d'une session SOL dans la console de ligne de commande iDRAC7

Utilisation de SOL depuis OpenSSH ou Telnet sur Linux

Pour démarrer SOL depuis OpenSSH ou Telnet sur une station de gestion Linux :

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente par défaut des sessions SSH ou Telnet dans **Présentation → Paramètres iDRAC → Réseau → Services**.

1. Démarrez un shell.
2. Connectez vous à iDRAC7 en utilisant la commande suivante :

   – Pour SSH: ssh *<adresse IP iDRAC7>* -l *<nom de connexion>*
   – Pour Telnet: telnet *<adresse IP iDRAC7>*

   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 l'une des commandes suivantes depuis l'invite de commande pour démarrer SOL :

   - `connect`
   - `console com2`

   Elle permet de connecter iDRAC7 au port SOL du système géré. Une fois la session SOL établie, la console de ligne de commande iDRAC7 n'est pas disponible. Suivez la séquence d'échappement correctement pour ouvrir la console de ligne de commande iDRAC7. La séquence d'échappement s'affiche également dès qu'une session SOL est connectée. Lorsque le système géré est arrêté, l'établissement de la session SOL prend un certain temps.

   REMARQUE : Vous pouvez utiliser la console com1 ou la console com2 pour démarrer le SOL. Redémarrez le serveur pour établir la connexion.

   La commande `console -h com2` affiche le contenu du tampon de l'historique série avant d'attendre une entrée à partir du clavier ou de nouveaux caractères du port série.

   La taille par défaut (et maximale) du tampon de l'historique est de 8 192 caractères. Vous pouvez définir une plus petite valeur en utilisant la commande suivante :

   `racadm config -g cfgSerial -o cfgSerialHistorySize <numéro>`
4. Quittez la session SOL pour fermer une session SOL active.

Liens connexes

Utilisation de la console virtuelle Telnet
Configuration de la touche Retour arrière de la session Telnet
Déconnexion d'une session SOL dans la console de ligne de commande iDRAC7

Utilisation de la console virtuelle Telnet

Certains clients Telnet sur les systèmes d'exploitation Microsoft peuvent ne pas afficher correctement l'écran de configuration du BIOS lorsque la console virtuelle du BIOS est configurée pour l'émulation VT100/VT220. Dans ce cas, faites passer la console du BIOS en mode ANSI pour mettre à jour l'affichage. Pour exécuter cette opération dans le menu de configuration du BIOS, sélectionnez **Console virtuelle → Type de terminal distant → ANSI**.

Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console virtuelle redirigée sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement ; sinon, certains écrans de texte risquent d'être illisibles.

Pour utiliser la console virtuelle Telnet :

1. Activez **Telnet** dans **Services du composant Windows.**
2. Connectez-vous à iDRAC7 en utilisant la commande `telnet <Adresse IP>:<numéro de port>`, où `Adresse IP` est l'adresse IP d'iDRAC7 et `numéro de port` est le numéro de port Telnet (si vous utilisez un nouveau port).

Configuration de la touche Retour arrière de la session Telnet

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

Pour configurer une session Linux Telnet pour qu'elle utilise la touche <Retour arrière>, ouvrez une invite de commande et tapez `stty erase ^h`. Dans l'invite, tapez `telnet`.

Pour configurer les clients Microsoft Telnet pour qu'ils utilisent la touche <Retour arrière> :

1. Ouvrez une fenêtre d'invite de commande (si nécessaire).
2. Si vous n'exécutez pas une session Telnet, tapez `telnet`. Si vous utilisez une session Telnet, appuyez sur `<Ctrl><]>`.

3. Depuis l'invite, tapez `set bsasdel`.

   Le message `La touche Retour arrière sera envoyée comme suppression` s'affiche.

Déconnexion d'une session SOL dans la console de ligne de commande iDRAC7

Les commandes de déconnexion d'une session SOL reposent sur l'utilitaire. Vous pouvez quitter l'utilitaire uniquement lorsqu'une session SOL est complètement terminée.

Pour déconnecter une session SOL, fermez la session SOL à partir de la console de ligne de commande d'iDRAC7.

- Pour quitter la redirection SOL, appuyez sur <Entrée>, <Échap>, puis sur <t>. La session SOL se ferme.
- Pour quitter une session SOL depis Telnet sur Linux, appuyez sur <Ctrl>+] et maintenez les touches enfoncées. Une invite Telnet s'affiche. Entrez `quit` pour quitter Telnet.
- Si une session SOL n'est pas terminée complètement dans l'utilitaire, d'autres sessions SOL peuvent ne pas être disponibles. Pour résoudre le problème, terminez la console de ligne de commande dans l'interface Web sous **Présentation générale** → **Paramètres iDRA** → **Sessions**.

Communication avec iDRAC7 en utilisant IPMI sur LAN

Vous devez configurer IPMI sur LAN pour iDRAC7 pour activer ou désactiver les commandes IPMI sur les canaux LAN vers des systèmes externes. S'il n'est pas configuré, les systèmes externes ne peuvent pas communiquer avec le serveur iDRAC7 en utilisant des commandes IPMI.

Configuration d'IPMI sur le LAN en utilisant l'interface Web

Pour configurer IPMI sur le LAN :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau**.

   La page **Réseau** s'affiche.
2. Sous les **paramètres IPMI**, définissez les valeurs des attributs et cliquez sur **Appliquer**.

   Pour plus d'informations sur les options, voir l'*aide en ligne d'DRAC7*.

   Les paramètres IPMI sur le LAN sont définis.

Configuration d'IPMI sur le LAN en utilisant l'utilitaire de configuration d'iDRAC

Configurez IPMI sur le LAN :

1. Dans l'**Utilitaire de configuration iDRAC**, accédez à **Réseau**.

   La page **Paramètres réseau iDRAC** s'affiche.
2. Définissez les valeurs des **Paramètres PMI**.

   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

   Les paramètres IPMI sur le LAN sont définis.

Configuration d'IPMI sur le LAN à l'aide de l'interface RACADM

Pour configurer IPMI sur le LAN avec la commande **set** ou **config** :

1. Activer IPMI sur le LAN :
   - Avec la commande **config** : `racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1`
   - Avec la commande **set** : `racadm set iDRAC.IPMILan.Enable 1`

   REMARQUE : Ce paramètre détermine les commandes IPMI exécutées en utilisant l'interface IPMI sur le LAN. Pour plus d'informations, voir les spécifications IPMI 2.0 sur le site **intel.com**.
2. Mettez à jour les privilèges du canal IPMI :
   - Avec la commande **config** : `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <niveau>`
   - Avec la commande **set** : `racadm set iDRAC.IPMILan.PrivLimit <niveau>`

   où `<niveau>` correspond à l'une des valeurs suivantes : 2 (Utilisateur), `3` (Opérateur) ou `4` (Administrateur)
3. Définissez la clé de cryptage du canal LAN IPMI, si nécessaire :
   - Avec la commande **config** : `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clé>`
   - Avec la commande **set** : `racadm set iDRAC.IPMILan.EncryptionKey <clé>`

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

   REMARQUE : iDRAC7 IPMI prend en charge le protocole RMCP+. Pour plus d'informations, voir les spécifications IPMI 2.0 sur le site **intel.com**.

Activation ou désactivation de l'interface distance RACADM

Vous pouvez activer ou désactiver l'interface RACADM en utilisant l'interface Web d'iDRAC7 ou l'interface RACADM. Vous pouvez exécuter jusqu'à cinq sessions d'interface distante RACADM simultanément.

Activation ou désactivation de l'interface distante RACADM en utilisant l'interface Web

Pour activer ou désactiver l'interface distante RACADM :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → Services**.
   La page **Services** s'affiche.
2. Sous **RACADM distante**, sélectionnez **Activé**. Autrement, sélectionnez **Désactivé**.
3. Cliquez sur **Appliquer**.
   L'interface RACADM distante est activée ou désactivée en fonction de la sélection.

Activation ou désactivation de l'interface RACADM distante en utilisant RACADM

La capacité RACADM distante est activée par défaut. Si elle est désactivée, saisissez l'une des commandes suivantes :

- Avec la commande **config** : `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1`
- Avec la commande **set** : `racadm set iDRAC.Racadm.Enable 1`

Pour désactiver la capacité distante, saisissez l'une des commandes suivantes :

- Avec la commande **config** : `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0`
- Avec la commande **set** : `racadm set iDRAC.Racadm.Enable 0`

REMARQUE : Il est recommandé d'exécuter ces commandes sur le système local.

Désactivation de l'interface locale RACADM

Par défaut, l'interface locale RACADM est activée. Pour la désactiver, voir Désactivation de l'accès pour modifier les paramètres de configuration d'iDRAC7 sur le système hôte.

Activation d'IPMI sur un système géré

Sur un système géré, utilisez Dell Open Manage Server Administrator pour activer ou désactiver IPMI. Pour plus d'informations, voir le *Dell Open Manage Server Administrator's User Guide* (Guide d'utilisation de l'utilitaire Dell OpenManage Server Administrator) à l'adresse **dell.com/support/manuals**.

Configuration de Linux pour la console série pendant le démarrage

Les étapes suivantes sont spécifiques de GRUB (Linux GRand Unified Bootloader). Des modification similaires sont nécessaires si un chargeur de démarrage différent est utilisé.

REMARQUE : Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console virtuelle redirigée, sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement. Sinon, certains écrans de texte risquent d'être illisibles.

Modifiez le fichier **/etc/grub.conf** de la manière suivante :

1. Localisez les sections Paramètres généraux dans le fichier et ajoutez :
   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```
2. Ajoutez deux options à la ligne du noyau :
   ```
   kernel ..... console=ttyS1,115200n8r console=tty1
   ```
3. Désactivez l'interface graphique de GRUB et utilisez l'interface texte. Autrement, l'écran GRUB ne s'affiche pas dans la console virtuelle RAC. Pour désactiver l'interface graphique, mettez en commentaire la ligne qui commence par `splashimage`.

   L'exemple suivant porte sur un fichier **/etc/grub.conf** qui illustre les modifications décrites dans cette procédure.

   ```
   # grub.conf generated by anaconda # Notez qu'il est inutile d'exécuter de
   nouveau grub après modification de ce fichier # REMARQUE : il est inutile
   de disposer d'une partition /boot. Ceci implique que tous les chemins #
   kernel et initrd sont relatifs à /, ex. # root (hd0,0) # kernel /boot/
   vmlinuz-version ro root=/dev/sdal # initrd /boot/initrd-version.img
   #boot=/dev/sda default=0 timeout=10 #splashimage=(hd0,2)/grub/splash.xpm.gz
   serial --unit=1 --speed=57600 terminal --timeout=10 serial title Red Hat
   Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /boot/
   vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
   console=ttyS1,115200n8r initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
   Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/
   vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s initrd /boot/initrd-2.4.9-e.3,im
   ```
4. Pour activer plusieurs options GRUB afin de démarrer des sessions de console virtuelle via la connexion RAC série, ajoutez les lignes suivantes à toutes les options :
   ```
   console=ttyS1,115200n8r console=tty1
   ```
   Dans l'exemple, `console=ttyS1,57600` a été ajouté à la première option.

Activation de l'ouverture de session dans la console virtuelle après le démarrage

Dans le fichier **/etc/inittab**, ajoutez une nouvelle ligne pour configurer `agetty` sur le port série COM2 :

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

L'exemple suivant montre un fichier avec la nouvelle ligne.

```
#inittab Ce fichier explique comment le processus INIT doit définir #le système
dans un niveau d'exécution. #Auteur :Miquel van Smoorenburg #Modifié pour RHS
Linux par Marc Ewing et Donnie Barnes #Niveau d'exécution par défaut. Les
niveaux d'exécution utilisés par RHS sont  : #0 - halt (N'AFFECTEZ PAS cette
valeur à initdefault) #1 - Mode mono-utilisateur #2 - Multi-utilisateur sans
NFS (Identique à 3, si vous n'avez pas #de mise en réseau) #3 - Mode multi-
utilisateur complet #4 - inutilisé #5 - X11 #6 - reboot (N'AFFECTEZ PAS cette
valeur à set initdefault) id:3:initdefault: #Initialisation du système.
si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/
rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/
rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 #Élément à exécuter
dans chaque niveau d'exécution. ud::once:/sbin/update ud::once:/sbin/update
#Trap CTRL-ALT-DELETE ca::ctrlaltdel:/sbin/shutdown -t3 -r now #Lorsque l'unité
d'alimentation UPS indique une erreur d'alimentation, supposez que nous
disposons encore de quelques #d'alimentation. Planifiez un arrêt dans 2 minutes
à partir de maintenant #Naturellement, cela suppose que l'alimentation est
installée et que #l'unité d'alimentation UPS est connectée et fonctionne
correctement. pf::powerfail:/sbin/shutdown -f -h +2 "Erreur d'alimentation ;
arrêt du système" #Si l'alimentation est rétablie avant l'arrêt, annulez-le. pr:
12345:powerokwait:/sbin/shutdown -c "Alimentation rétablie ; arrêt annulé"

#Exécutez gettys dans les niveaux d'exécution standard co:2345:respawn:/sbin/
agetty -h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2 3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4 5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6 #Run xdm in runlevel 5 #xdm est désormais un
service distinct x:5:respawn:/etc/X11/prefdm -nodaemon
```

Dans le fichier**/etc/securetty**, ajoutez une ligne avec le nom du terminal série tty pour COM2:

```
ttyS1
```

L'exemple suivant montre un fichier avec la nouvelle ligne.

REMARQUE : Uutilisez la séquence de touches d'arrêt (~B) pour exécuter les commandes de touches **Magic SysRq** Linux sur une console série à l'aide de l'outil IPMI.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```

Schémas cryptographiques SSH pris en charge

Pour communiquer avec iDRAC7 en utilisant le protocole SSH, iDRAC7 prend en charge les schémas cryptographiques répertoriés dans le tableau suivant.

Tableau 12. Schémas cryptographiques SSH

Type de schéma	Schéma
Cryptographie asymétrique	Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 conformément au NIST
Cryptographie symétrique	• AES256-CBC

Type de schéma	Schéma
	• RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Intégrité du message	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentification	Mot de passe
Authentication PKA	Paires de clés publique et privée

Utilisation de l'authentification par clé publique pour SSH

iDRAC7 prend en charge l'authentification par clé publique (PKA) sur SSH. Cette fonction est disponible sous licence. Lorsque PKA sur SSH est configuré et utilisé correctement, vous n'avez pas à entrer le nom d'utilisateur et le mot de passe lorsque vous ouvrez une session dans iDRAC7. Ceci est pratique pour définir des scripts automatiques qui exécutent diverses fonctions. Les clés mises à jour doivent avoir le format RFC 4716 ou openssh. Autrement vous devez les convertir dans ce format.

Quel que soit le cas, une paire de clés privée et publique doit être générée sur la station de gestion. La clé publique est téléversée vers l'utilisateur local iDRAC7 et la clé privée est utilisée par le client SSH pour établir la relation de confiance entre la station de gestion et iDRAC7.

Vous pouvez générer la paire de clés publique et privée à l'aide de :

- l'application *PuTTY Key Generator* pour les clients Windows ;
- l'interface CLI *ssh-keygen* pour les clients Linux.

PRÉCAUTION : Ce privilège est normalement réservé aux utilisateurs membres du groupe d'utilisateurs Administrateur sur iDRAC7. Toutefois, les utilisateurs dans le groupe d'utilisateurs « Personnalisé » peuvent recevoir ce privilège. Un utilisateur avec ce privilège peut modifier n'importe quelle configuration d'utilisateur. Ceci inclut la création ou la suppression d'un utilisateur, la gestion des clés SSH des utilisateurs, etc. Par conséquent, affectez ce privilège avec précaution.

PRÉCAUTION : La possibilité de téléverser, afficher et supprimer des clés SSH repose sur le privilège utilisateur de configuration d'utilisateurs. Ce privilège permet aux utilisateurs de configurer la clé SSH d'un autre utilisateur. Par conséquent, affectez ce privilège avec précaution.

Génération de clés publiques pour Windows

Pour utiliser l'application *PuTTY Key Generator* pour 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). Les algorithmes de génération de clé compatibles sont RSA et DSA uniquement.
2. Entrez le nombre de bits de la clé. Pour RSA, il doit être compris entre 768 et 4 096 bits et pour DSA, il doit être de 1 024 bits.

3. Cliquez sur **Générer** et déplacez la souris dans la fenêtre en suivant les instructions.
   Les clés sont générées.
4. Vous ne pouvez pas modifier le champ de commentaire de la clé.
5. Entrez une phrase secrète pour protéger la clé.
6. Enregistrez la clé publique et la clé privée.

Génération de clés publiques pour Linux

Pour utiliser l'application *ssh-keygen* pour créer la clé de base, ouvrez une fenêtre de terminal et dans l'invite du shell, entrez `ssh-keygen –t rsa –b 1024 –C testing`

où :

- `–t` correspond à *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 ; l'option est facultative.

REMARQUE : Les options sont sensibles à la casse.

Suivez les instructions. Après l'exécution de la commande, téléversez le fichier public.

PRÉCAUTION : Les clés générées depuis la station de gestion Linux en utilisant ssh-keygen n'ont pas le format 4716. Convertissez les clés dans le format 4716 en utilisant `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Ne changez pas les autorisations du fichiers de clé. La conversion doit être effectuée en utilisant les autorisations par défaut.

REMARQUE : iDRAC7 ne prend pas en charge le transfert des clés via ssh-agent.

Téléversement de clés SSH

Vous pouvez téléverser jusqu'à quatre clés publiques *par utilisateur* pour les utiliser sur une interface SSH. Avant d'ajouter les clés publiques, veillez à les visualiser si elles sont configurées afin de ne pas les remplacer accidentellement.

Lorsque vous ajoutez de nouvelles clés, vérifiez que les clés existantes ne se trouvent pas dans l'index auquel la nouvelle clé est ajoutée. iDRAC7 ne vérifie pas que les clés précédentes sont supprimées avant d'ajouter les nouvelles clés. Lorsque vous ajoutez une nouvelle clé, vous pouvez l'utiliser si l'interface SSH est activée.

Téléversement des clés SSH à l'aide de l'interface Web

Pour téléverser des clés SSH :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Réseau → Authentification des utilisateurs → Utilisateurs locaux**.
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configurations de clés SSH**, sélectionnez **Téléverser une ou des clés SSH**, puis cliquez sur **Suivant**.
   La page **Téléverser une ou des clés SSH** s'affiche.
4. Téléversez les clés SSH de l'une des manières suivantes :
   - Téléversez le fichiers de clé.
   - Copiez le contenu du fichier de clé dans zone de texte.

   Reportez-vous à l'aide en ligne d'IDRAC 7 pour plus d'informations.

5. Cliquez sur **Appliquer**.

Téléversement des clés SSH à l'aide de l'interface RACADM

Pour télécharger les clés SSH, exécutez a commande suivante :

REMARQUE : vous ne pouvez pas téléverser et copier une clé simultanément.

- Pour l'interface locale RACADM : `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <nom de fichier>`
- Pour l'interface distance RACADM en utilisant Telnet ou SSH : `racadm sshpkauth -i <2 à 16> -k <1 à 4> -t <texte clé>`

Par exemple, pour téléverser une clé valide vers l'ID d'utilisateur iDRAC7 2 dans l'espace de la première clé en utilisant un fichier, exécutez la commande suivante :

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

REMARQUE : L'option `-f` n'est pas prise en charge dans l'interface RACADM telnet/ssh/série.

Affichage des clés SSH

Vous pouvez afficher les clés téléversées vers iDRAC7.

Affichage des clés SSH en utilisant l'interface Web

Pour afficher les clés SSH :

1. Dans l'interface Web, accédez à **Présentation → Paramètres iDRAC → Réseau → Authentification des utilisateurs → Utilisateurs locaux** .
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configuration de clé SSH** sélectionnez **Afficher/Supprimer une ou des clés SSH**, puis cliquez sur **Suivant**.
   La page **Afficher/Supprimer une ou des clés SSH** s'affiche avec les détails des clés.

Affichage des clés SSH en utilisant l'interface RACADM

Pour afficher les clés SSH, exécutez les commandes suivantes :

- Pour une clé spécifique : `racadm sshpkauth -i <2 à 16> -v -k <1 à 4>`
- Pour toutes les clés : `racadm sshpkauth -i <2 à 16> -v -k all`

Suppression des clés SSH

Avant de supprimer des clés publiques, affichez les clés si elles sont définies afin de ne pas les supprimer par inadvertance.

Supprression de clés SSH en utilisant l'interface Web

Pour supprimer des clés SSH :

1. Dans l'interface Web, accédez à **Overview → iDRAC Settings → Network → User Authentication → Local Users** (Présentation, Paramètres iDRAC, Réseau, Authentification des utilisateurs, Utilisateurs locaux).
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.

3. Sous **SSH Key Configurations**, sélectionnez **View/Remove SSH Key(s)** (Afficher/Supprimer une ou des clés SSH) et cliquez sur **Suivant**.

   La page **View/Remove SSH Key(s) (Afficher/Supprimer une ou des clés SSH)** affiche les détails des clés.
4. Sélectionnez **Remove for the key(s) you want to delete**, (Supprimer la ou clés désirées), puis cliquez sur **Appliquer**.

   Les clés sélectionnées sont supprimées.

Suppression des clés SSH en utilisant l'interface RACADM

Pour supprimer les clés SSH, exécutez les commandes suivantes :

- Pour une clé spécifique : `racadm sshpkauth -i <2 à 16> -d -k <1 à 4>`
- Pour toutes les clés : `racadm sshpkauth -i <2 à 16> -d -k all`

7

Configuration des comptes et des privilèges des utilisateurs

Vous pouvez configurer des comptes d'utilisateur avec des privilèges spécifiques (*droit basé sur un rôle*) pour gérer le système en utilisant iDRAC7 et maintenir la sécurité du système. Par défaut, iDRAC7 est configuré avec un compte d'administrateur local. Ce nom par défaut est *root* et le mot de passe, *calvin*. En tant qu'administrateur, vous pouvez configurer des comptes d'utilisateur pour autoriser d'autres utilisateurs à accéder à iDRAC7.

Vous pouvez définir des utilisateurs locaux ou utiliser des services d'annuaire, tels que Microsoft Active Directory ou LDAP, pour définir des comptes d'utilisateur. L'utilisation d'un service d'annuaire permet de disposer d'un emplacement central de gestion des comptes d'utilisateur autorisés.

iDRAC7 prend en charge l'accès à base de rôle pour utilisateurs avec un groupe de privilèges associés. Les rôles sont Administrateur, Opérateurs, Lecture seule et Aucun. Le rôle définit les privilèges maximaux disponibles.

Liens connexes

Configuration des utilisateurs locaux
Configuration des utilisateurs d'Active Directory
Configuration des utilisateurs LDAP générique

Configuration des utilisateurs locaux

Vous pouvez configurer jusqu'à 16 utilisateurs locaux dans iDRAC7 avec des autorisations d'accès spécifiques. Avant de créer un utilisateur iDRAC7, vérifiez s'il existe des utilisateurs. Vous pouvez définir le nom, le mot de passe et des rôles avec des privilèges pour ces utilisateurs. Les noms d'utilisateur et les mots de passe peuvent être modifiés à l'aide de n'importe quelle interface sécurisée iDRAC7 (à savoir, l'interface Web, RACADM ou WS-MAN). Vous pouvez également activer ou désactiver l'authentification SNMPv3 pour chaque utilisateur.

REMARQUE : La fonction SNMPv3 est sous licence et disponible avec la licence iDRAC7 Enterprise.

Configuration des utilisateurs locaux en utilisant l'interface Web d'iDRAC7

Pour ajouter et configurer les utilisateurs iDRAC7 locaux :

REMARQUE : vous devez disposer de l'autorisation Configurer des utilisateurs pour pouvoir configurer un utilisateur iDRAC7.

1. Dans l'interface Web d'iDRAC7 accédez à **Présentation générale → Paramètres iDRAC → Authentification des utilisateurs → Utilisateurs locaux.**

   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.

   REMARQUE : L'utilisateur 1 est réservé à l'utilisateur anonyme IPMI ; vous ne pouvez pas changer cette configuration.

   La page **Menu principal utilisateur** s'affiche.
3. Sélectionnez **Configurer**, puis cliquez sur **Suivant**.

   La page **Configuration de l'utilisateur** s'affiche.

4. Activez l'ID utilisateur et spécifiez le nom d'utilisateur, le mot de passe et les droits d'accès de l'utilisateur. Vous pouvez également activer l'authentification SNMPv3 pour cet utilisateur. Pour en savoir plus sur les options, voir *iDRAC7 Online Help* (Aide en ligne iDRAC7).
5. Cliquez sur **Appliquer**. L'utilisateur est créé avec les privilèges demandés.

Configuration des utilisateurs locaux en utilisant l'interface RACADM

REMARQUE : Vous devez ouvrir une session en tant qu'utilisateur **root** pour pouvoir exécuter des commandes RACADM sur un système Linux distant.

Vous pouvez configurer un seul ou plusieurs utilisateurs iDRAC7 en utilisant l'interface RACADM.

Pour configurer plusieurs utilisateurs iDRAC7 avec des paramètres de configuration identiques, exécutez l'une des procédures suivantes :

- Utilisez les exemples RACADM indiqués dans cette section comme modèle pour créer un fichier séquentiel de commandes RACADM, puis exécutez ce fichier sur chaque système géré.
- Créez le fichier de configuration iDRAC7 et exécutez la sous-commande **racadm config** ou **racadm set** sur chaque système géré en utilisant le même fichier de configuration.

Si vous configurez un nouveau iDRAC7 ou que vous avez utilisé la commande **racadm racresetcfg**, le seul utilisateur en cours est `root` avec le mot de passe `calvin`. La sous-commande **racresetcfg** restaure les valeurs par défaut d'iDRAC7.

REMARQUE : Les utilisateurs peuvent être activés et désactivés ensuite. Par conséquent, un utilisateur peut avoir un numéro d'index différent dans chaque iDRAC7.

Pour déterminer si un utilisateur existe, tapez une des commandes suivantes à l'invite de commande :

- Avec la commande **config** : `racadm getconfig –u <nom_d'utilisateur>`
- Avec la commande **get** : `racadm get —u <nom_d'utilisateur>`

OU

Tapez la commande suivante une fois pour chaque index (de 1 à 16) :

- Avec la commande **config** : `racadm getconfig –g cfgUserAdmin –i <index>`
- Avec la commande **get** : `racadm get iDRAC.Users.<index>.UserName`

REMARQUE : Vous pouvez également taper `racadm getconfig –f <myfile.cfg>` ou `racadm get –f <myfile.cfg>` et afficher ou modifier le fichier **myfile.cfg**, ce qui inclut tous les paramètres de configuration iDRAC7.

Plusieurs paramètres et ID d'objet sont affichés avec leurs valeurs actuelles. Les objets importants sont les suivants :

- Si vous avez utilisé la commande **getconfig** :
  ```
  # cfgUserAdminIndex=XX

  cfgUserAdminUserName=
  ```
- Si vous avez utilisé la commande **get** :
  ```
  iDRAC.Users.UserName=
  ```

Si l'objet **cfgUserAdminUserName** n'a pas de valeur, le numéro d'index, indiqué par l'objet **cfgUserAdminIndex**, peut être utilisé. Si un nom est affiché après « = », cet index est pris par ce nom d'utilisateur.

Lorsque vous activez ou désactivez manuellement un utilisateur avec la sous-commande **racadm config**, vous *devez* spécifier l'index avec l'option **-i**.

Notez que l'objet **cfgUserAdminIndex** dans l'exemple précédent contient le caractère « # »'. Il indique qu'il s'agit d'un objet en lecture seule. En outre, si vous utilisez la commande **racadm config -f racadm.cfg** pour définir un nombre de

groupes/objets à écrire, l'index ne peut pas être spécifié. Ce comportement offre une plus grande souplesse pour configurer plusieurs iDRAC7 avec les mêmes paramètres.

Ajout d'un utilisateur iDRAC7 à l'aide de l'interface RACADM

Pour ajouter un nouvel utilisateur à la configuration RAC, procédez comme suit :

1. Définissez le nom de l'utilisateur.
2. Définissez le mot de passe.
3. Spécifiez les privilèges d'utilisateur suivants :
   - iDRAC7
   - LAN
   - Port série
   - Communications série sur le LAN
4. Activez l'utilisateur.

Exemple :

L'exemple suivant explique comment ajouter le nouvel utilisateur « Jean » avec le mot de passe « 123456 » et les privilèges LOGIN à RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 jean

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 123456

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiLanPrivilege 2

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiSerialPrivilege 2

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminEnable 1
```

Pour vérifier, utilisez l'une des commandes suivantes :

```
racadm getconfig -u jean

racadm getconfig –g cfgUserAdmin –i 3
```

Pour plus d'informations sur les commandes RACADM, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC), disponible à l'adresse **dell.com/support/manuals**.

Activation d'un utilisateur iDRAC7 avec des droits

Pour activer un utilisateur avec des droits (droit basé sur un rôle) :

REMARQUE : Vous pouvez utiliser les commandes **getconfig** et **config** ou les commandes **get** et **set**.

1. recherchez un index d'utilisateur disponible en utilisant la commande suivante :
   - Avec la commande **getconfig** : `racadm getconfig -g cfgUserAdmin -i <index>`
   - Avec la commande **get** : `racadm get iDRAC.Users <index>`

2. Tapez les commandes suivantes avec les nouveaux nom d'utilisateur et mot de passe.
   - Avec la commande **config** : `racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <user privilege bitmask value>`
   - Avec la commande **set** : `racadm set iDRAC.Users.<index>.Privilege <valeurs de masque binaire de privilèges utilisateur>`

   REMARQUE : Pour consulter la liste des valeurs de masque binaire de privilèges utilisateur spécifiques, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC), disponible sur le site **dell.com/support/manuals**. La valeur de privilège par défaut (0) indique que l'utilisateur n'a aucun privilège.

Configuration des utilisateurs d'Active Directory

Si votre société utilise le logiciel Microsoft Active Directory, vous pouvez le configurer pour fournir l'accès à iDRAC7, ce qui permet d'ajouter des privilèges iDRAC7 aux utilisateurs existants et de les contrôler dans le service d'annuaire. Cette fonction est disponible sous licence.

REMARQUE : L'utilisation d'Active Directory pour la reconnaissance des utilisateurs iDRAC7 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 Active Directory pour l'ouverture de session dans iDRAC7. Vous pouvez également fournir des droits basés sur un rôle pour qu'un administrateur puisse configurer des privilèges pour chaque utilisateur.

Les noms de rôle et de privilège iDRAC7 ont changé par rapport à la génération précédente de serveurs. Les noms des rôles sont les suivants

Tableau 13. Rôles iDRAC7

Génération en cours	Génération antérieure	Privilèges
Administrateur	Administrateur	Connexion, Configurer, Configurer des utilisateurs, Journaux, Contrôler le système, Accéder à la console virtuelle, Accéder à Média Virtuel, Opérations système, Déboguer
Opérateur	Utilisateur privilégié	Connexion, Configurer, Configurer des utilisateurs, Journaux, Contrôler le système, Accéder à la console virtuelle, Accéder à Média Virtuel, Opérations système, Déboguer
Lecture seule	Utilisateur invité	Connexion
Aucun	Aucun	Aucun

Tableau 14. Privilèges d'utilisateur iDRAC7

Génération en cours	Génération antérieure	Description
Connexion	Connexion à iDRAC	Permet à l'utilisateur de se connecter à iDRAC.
Configurer	Configurer iDRAC	Permet à l'utilisateur de configurer iDRAC.

Génération en cours	Génération antérieure	Description
Configurer des utilisateurs	Configurer des utilisateurs	Donne la possibilité à l'utilisateur d'autoriser des utilisateurs à d'accéder au système.
Journaux	Effacer les journaux	Permet à l'utilisateur d'effacer uniquement le journal des événements système (SEL).
Contrôle du système	Exécuter les commandes de contrôle du serveur	Permet d'effectuer un cycle d'alimentation sur le système hôte.
Accéder à la console virtuelle	Accéder à la redirection de la console (pour les serveurs lames) Accéder à la console virtuelle (pour les serveurs en rack et tour)	Permet à l'utilisateur d'exécuter la console virtuelle.
Accéder à Média Virtuel	Accéder à Média Virtuel	Permet à l'utilisateur d'exécuter et d'utiliser Média Virtuel.
Opérations système	Alertes de test	Autorise les événements initialisés et générés par l'utilisateur, et les informations sont envoyées en tant que notification asynchrone et journalisés.
Debug (Débogage)	Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Liens connexes

Conditions d'utilisation de l'authentification Active Directory d'iDRAC7

Mécanismes d'authentification Active Directory pris en charge

Conditions d'utilisation de l'authentification Active Directory d'iDRAC7

Pour utiliser la fonction d'authentification Active Directory d'iDRAC7, vérifiez que vous avez :

- Déployé une infrastructure Active Directory. Voir le site Web Microsoft pour plus d'informations.
- Intégré PKI à l'infrastructure Active Directory. iDRAC7 utilise le mécanisme d'infrastructure de clé publique (PKI) standard pour s'authentifier en toute sécurité dans Active Directory. Voir le site Web Microsoft pour plus d'informations.
- Activé SSL (Secure Socket Layer (SSL) dans tous les contrôleurs de domaines auxquels iDRAC7 se connecte pour l'authentification dans tous les contrôleurs de domaines.

Liens connexes

Activation de SSL dans un contrôleur de domaine

Activation de SSL dans un contrôleur de domaine

Lorsque iDRAC7 authentifie les utilisateurs avec un contrôleur de domaine Active Directory, il démarre une session SSL avec le contrôleur de domaine. À ce stade, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (CA) dont le certificat racine est également téléversé vers iDRAC7. Pour qu'iDRAC7 puisse s'authentifier auprès d'*un* contrôleur de domaine, qu'il s'agisse du contrôleur de domaine racine ou enfant, le contrôleur de domaine doit avoir un certificat SSL signé par l'autorité de certification du domaine.

Si vous utilisez Autorité de certification racine d'entreprise Microsoft pour affecter *automatiquement* tous les contrôleurs de domaine à un certificat SSL, vous devez :

1. installer le certificat SSL dans chaque contrôleur de domaine ;
2. exporter le certificat CA racine du contrôleur de domaine vers iDRAC7 ;

3. importer le certificat SSL du micrologiciel d'iDRAC7.

Liens connexes

Installation du certificat SSL pour chaque contrôleur de domaine
Exportation du certificat d'autorité de certification (CA) du contrôleur de domaine vers iDRAC7
Importation du certificat SSL du micrologiciel d'iDRAC7

Installation du certificat SSL pour chaque contrôleur de domaine

Pour installer le certificat SSL pour chaque contrôleur de domaine :

1. Cliquez sur **Démarrer** → **Outils d'administration** → **Stratégie du domaine de sécurité** .
2. Développez le dossier **Règles de clé publique**, cliquez avec le bouton droit de la souris sur **Paramètres de demande automatique de certificat** et cliquez sur **Demande automatique de certificat**.

   L'**Assistant Demande automatique de certificat** s'affiche.
3. Cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.
4. Cliquez sur **Suivant** et sur **Terminer**. Le certificat SSL est installé.

Exportation du certificat d'autorité de certification (CA) du contrôleur de domaine vers iDRAC7

REMARQUE : Si votre système fonctionne sous Windows 2000 ou que vous utilisez une autorité de certification autonome, les étapes suivantes peuvent être différentes.

Pour exporter le certificat CA racine du contrôleur de domaine vers iDRAC7 :

1. Localisez le contrôleur de domaine qui exécute le service CA d'entreprise Microsoft.
2. Cliquez sur **Démarrer** → **Exécuter**.
3. Tapez `mmc` et cliquez sur **OK**.
4. Dans la fenêtre **Console 1** (MMC), cliquez sur **Fichier (**ou sur **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 **Ordinateur** et cliquez sur **Suivant**.
8. Sélectionnez **Ordinateur local** et cliquez sur **Terminer**, puis sur **OK**.
9. Dans la fenêtre de **Console 1**, accédez au dossier **Certificats Personnel Certificats**.
10. Recherchez le certificat d'autorité de certification racine et cliquez dessus avec le bouton droite de la souris, sélectionnez **Toutes les tâches** et cliquez sur **Exporter...**
11. Dans l'**Assistant Exportation de certificat**, cliquez sur **Suivant** et sélectionnez **Ne pas exporter la clé privée**.
12. Cliquez sur **Suivant** et sélectionnez **Codé en base 64 X.509 (.cer)** comme format.
13. Cliquez sur **Suivant** et enregistrez le certificat dans un répertoire de votre système.
14. Téléversez vers iDRAC7 le certificat que vous avez enregistré au cours de l'étape 13.

Importation du certificat SSL du micrologiciel d'iDRAC7

Le certificat SSL iDRAC7 est identique au certificat utilisé pour le serveur Web d'iDRAC7. Tous les contrôleurs iDRAC7 sont fournis avec un certificat autosigné par défaut.

Si le serveur Active Directory est configuré pour authentifier le client pendant l'initialisation de session SSL, vous devez téléverser le certificat du serveur iDRAC7 vers le contrôleur de domaine Active Directory. Cette opération supplémentaire n'est pas nécessaire si Active Directory n'authentifie pas le client pendant l'initialisation de la session SSL.

REMARQUE : Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

REMARQUE : Si le certificat SSL du micrologiciel d'iDRAC7 est signé par une autorité de certification et que le certificat de cette autorité se trouve déjà dans la liste des autorités de certification racines de confiance du contrôleur de domaine, n'exécutez pas les étapes de cette section.

Pour importer le certificat SSL du micrologiciel iDRAC7 vers toutes les listes de certificats de confiance du contrôleur de domaine :

1. Téléchargez le certificat SSL iDRAC7 SSL à l'aide de la commande RACADM suivante :
   ```
   racadm sslcertdownload -t 0x1 -f <certificat SSL RAC>
   ```
2. Sur le contrôleur de domaine, ouvrez une fenêtre .**Console MMC** et sélectionnez **Certificats** → **Autorités de certification racines de confiance**.
3. Cliquez avec le bouton droit de la souris sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
4. Cliquez sur **Suivant** et accédez au fichier de certificat SSL.
5. Installez le certificat SSL d'iDRAC7 dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

   Si vous avez installé votre propre certificat, vérifiez que l'autorité de certification signataire du certificat se trouve dans la liste des **autorités de certification racines de confiance**. Si elle n'y figure pas, vous devez l'installer sur tous les contrôleurs de domaine.
6. Cliquez sur **Suivant** et indiquez si vous voulez que Windows sélectionne automatiquement la banque de certificats en fonction du type de certificat ou bien naviguez vers une banque de votre choix.
7. Cliquez sur **Terminer** et sur **OK**. Le certificat SSL du micrologiciel d'iDRAC7 est importé vers les listes de certificats autorisés de tous les contrôleurs de domaine.

Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur iDRAC7 en utilisant deux méthodes :

- La solution de *schéma standard* qui utilise uniquement des objets du groupe Active Directory.
- *La solution de schéma étendu qui contient des objets Active Directory personnalisés. Tous les objets de contrôle d'accès sont gérés dans Active Directory. La solution offre une souplesse maximale pour configurer l'accès des utilisateurs dans différents iDRAC7 avec des niveaux de privilèges différents.*

Liens connexes

Présentation d'Active Directory avec le schéma standard
Présentation d'Active Directory avec schéma étendu

Présentation d'Active Directory avec le schéma standard

Comme indiqué dans l'illustration ci-dessous, l'utilisation du schéma standard pour l'intégration d'Active Directory nécessite une configuration dans Active Directory et dans iDRAC 7.

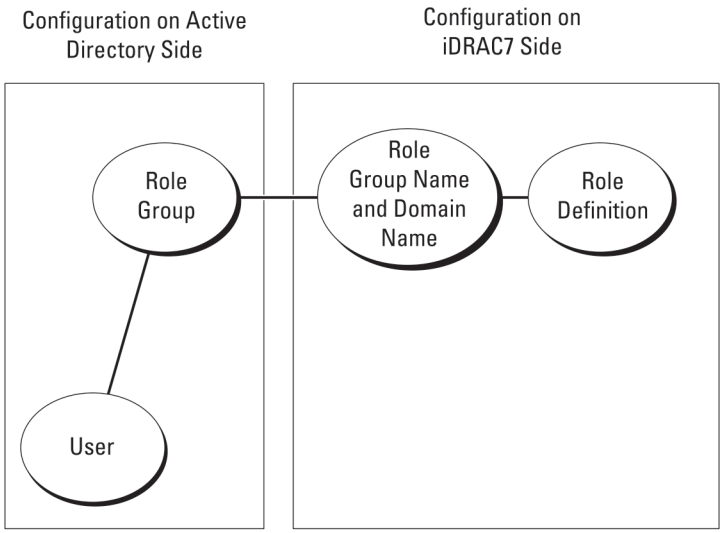

Figure 1. Configuration d'iDRAC7 avec le schéma standard Active Directory

Dans Active Directory, un objet Groupe standard est utilisé comme groupe de rôles. Un utilisateur qui dispose d'un accès iDRAC7 est membre du groupe de rôles. Pour que cet utilisateur puisse accéder à un iDRAC7, le nom du groupe de rôles et son nom de domaine doivent être définis dans l'iDRAC7. Le rôle et le niveau de privilège sont définis dans chaque iDRAC7 et non pas dans Active Directory. Vous pouvez définir jusqu'à cinq groupes de rôles dans chaque iDRAC7. Le tableau répertorie les privilèges par défaut des groupes de rôles.

Tableau 15. Privilèges par défaut des groupes de rôles

Groupes de rôles	Niveau de privilège par défaut	Droits accordées	Masque binaire
Groupe de rôles 1	Aucun	Ouvrir une session iDRAC, Configurer iDRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle de serveur, Accéder à la console virtuelle, Accès à Média Virtuel, Tester les alertes, Exécuter des commandes de diagnostic	0x000001ff
Groupe de rôles 2	Aucun	Ouvrir une session iDRAC, Configurer iDRAC, Exécuter des commandes de contrôle de serveur, Accéder à la console virtuelle, Accéder à Média Virtuel, Tester les alertes, Exécuter des commandes de diagnostic	0x000000f9
Groupe de rôles 3	Aucun	Ouvrir une session sur iDRAC	0x00000001
Groupe de rôles 4	Aucun	Aucun droit attribué	0x00000000
Groupe de rôles 5	Aucun	Aucun droit attribué	0x00000000

REMARQUE : Les valeurs Masque binaire sont utilisées uniquement lors de la définition du schéma standard avec l'interface RACADM.

Scénario impliquant un seul domaine et scénario impliquant plusieurs domaines

Si tous les utilisateurs et groupes de rôles, y compris les groupes imbriqués, se trouvent dans le même domaine, seules les adresses des contrôleurs de domaine doivent être définies dans iDRAC7. Dans ce scénario impliquant un seul domaine, n'importe quel type de groupe est pris en charge.

Si tous les utilisateurs et groupes de rôles, ou un groupe imbriqué, proviennent de plusieurs domaines, des adresses de serveur de catalogue global doivent être définies dans iDRAC7. Dans ce scénario impliquant plusieurs domaine, tous les groupes de rôles et les groupes imbriqués, s'il en existe, doivent être de type Groupe universel.

Configuration d'Active Directory avec le schéma standard

Pour configurer iDRAC7 pour ouvrir une session Active Directory :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le snap-in Utilisateurs et ordinateurs Active Directory.
2. Créez un groupe ou sélectionnez un groupe existant. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour accéder à iDRAC7.
3. Définissez le nom du groupe, le nom de domaine et les privièges de rôle dans iDRAC7 en utilisant l'interface Web ou RACADM d'iDRAC7.

Liens connexes

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC7
Configuration d'Active Directory avec le schéma standard à l'aide de l'interface RACADM

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC7

REMARQUE : Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC7*.

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Authentification des utilisateurs → Services d'annuaire → Microsoft Active Directory**.

   La page du **Résumé Active Directory** apparaît.
2. Cliquez sur **Configurer Active Directory**.

   La page **Configuration et gestion d'Active Directory - Étape 1 sur 4** s'affiche.
3. Vous pouvez également activer la validation de certificat et téléverser le certificat numérique signé par une autorité de certification, utilisé pendant l'initialisation des connexions SSL lors de la communication avec le serveur Active Directory (AD). Pour ce faire, vous devez définir les contrôleurs de domaine et le nom de domaine complet qualifié du catalogue. Vous le faites dans les étapes suivantes. Le DNS doit être alors configuré correctement dans les paramètres réseau.
4. Cliquez sur **Suivant**.

   La page **Configuration et gestion d'Active Directory -Étape 2 sur 4** s'affiche.
5. Activez Active Directory et définissez les informations d'emplacement des serveurs et des comptes d'utilisateur Active Directory. Définissez également le délai d'attente des réponses d'Active Directory qu'iDRAC7 doit respecter lors de l'ouverture de session dans iDRAC7.

   REMARQUE : Si la validation de certificat est activée, définissez les adresses de serveur de contrôleur de domaine et le nom de domaine complet qualifié du catalogue global. Vérifiez que le DNS est correctement configuré dans **Présentation générale → Paramètres iDRAC → Réseau**.
6. Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory -Étape 3 sur 4** s'affiche.

7. Sélectionnez **Schéma standard**, puis cliquez sur Suivant.

   La page **Configuration et gestion d'Active Directory - Étape 4a sur 4** s'affiche.
8. Entrez l'emplacement du ou des services de catalogue global Active Directory et définissez les groupes de privilèges utilisés pour autoriser les utilisateurs.
9. Cliquez sur **Groupe de rôles** pour configurer la stratégie d'autorisation de contrôle pour les utilisateurs qui se trouvent sous le mode de schéma standard.

   La page **Configuration et gestion d'Active Directory - Étape 4b sur 4** s'affiche.
10. Définissez les privilèges, puis cliquez sur **Appliquer**.

    Les paramètres sont appliqués et la page **Configuration et gestion d'Active Directory - Étape 4a sur 4** s'affiche.
11. Cliquez sur **Terminer**. Les paramètres Active Directory pour le schéma standard sont définis.

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface RACADM

Pour configurer iDRAC7 Active Directory avec le schéma standard en utilisant l'interface RACADM :

1. Depuis l'invite de commande racadm, exécutez les commandes suivantes :
   - Avec la commande **config** :

     ```
     racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
     cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -i
     <index> -o cfgSSADRoleGroupName <nom commun du groupe de rôles> racadm
     config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <nom de
     domaine complet> racadm config -g cfgStandardSchema -i <index> -o
     cfgSSADRoleGroupPrivilege <valeur de masque de bits pour des permissions
     RoleGroup spécifiques> racadm config -g cfgActiveDirectory -o
     cfgADDomainController1 <nom de domaine complet ou adresse IP du
     contrôleur de domaine> racadm config -g cfgActiveDirectory -o
     cfgADDomainController2 <nom de domaine complet ou adresse IP du
     contrôleur de domaine> racadm config -g cfgActiveDirectory -o
     cfgADDomainController3 <nom de domaine complet qualifié ou adresse IP du
     contrôleur de domaine> racadm config -g cfgActiveDirectory -o
     cfgADGlobalCatalog1 <nom de domaine complet qualifié ou adresse IP du
     contrôleur de domaine> racadm config -g cfgActiveDirectory -o
     cfgADGlobalCatalog2 <nom de domaine complet qualifié ou adresse IP du
     contrôleur de domaine> racadm config -g cfgActiveDirectory -o
     cfgADGlobalCatalog3 <nom de domaine complet qualifié ou adresse IP du
     contrôleur de domaine>
     ```

   - Avec la commande **set** :

     ```
     racadm set iDRAC.ActiveDirectory.Enable 1 racadm set
     iDRAC.ActiveDirectory.Schema 2 racadm set iDRAC.ADGroup.Name <nom commun
     du groupe de rôles> racadm set iDRAC.ADGroup.Domain <nom de domaine
     complet qualifié> racadm set iDRAC.ADGroup.Privilege <Valeur du masque de
     bits pour des permissions RoleGroup spécifiques> racadm set
     iDRAC.ActiveDirectory.DomainController1 <nom de domaine complet qualifié
     ou adresse IP du contrôleur de domaine> racadm set
     iDRAC.ActiveDirectory.DomainController2 <nom de domaine complet qualifié
     ou adresse IP du contrôleur de domaine> racadm set
     iDRAC.ActiveDirectory.DomainController3 <nom de domaine complet qualifié
     ou adresse IP du contrôleur de domaine> racadm set
     iDRAC.ActiveDirectory.GlobalCatalog1 <nom de domaine complet qualifié ou
     adresse IP du contrôleur de domaine> racadm set
     iDRAC.ActiveDirectory.GlobalCatalog2 <nom de domaine complet qualifié ou
     adresse IP du contrôleur de domaine> racadm set
     iDRAC.ActiveDirectory.GlobalCatalog3 <nom de domaine complet qualifié ou
     adresse IP du contrôleur de domaine>
     ```

     Pour les valeurs de masque binaire des autorisations Groupe de rôles, voir Privilège du groupe de rôles par défaut.

     Entrez le nom de domaine complet qualifié du contrôleur de domaine et non pas celui du domaine. Par exemple, entrez `nomserveur.dell.com` et non pas `dell.com`.

     Au moins une des trois adresses doit être définie. iDRAC7 tente de se connecter à chacune d'elles l'une après l'autre jusqu'à ce qu'il puisse établir une connexion. Avec le schéma standard, il s'agit des adresses des contrôleurs de domaine où se trouvent les comptes d'utilisateur et les groupes de rôles.

     Le serveur de catalogue global est uniquement nécessaire pour le schéma standard lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents. S'il existe plusieurs domaines, seul le groupe Universel peut être utilisé.

     Le nom de domaine complet qualifié ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.

Pour désactiver la validation de certificat durant l'établissement de liaison SSL, entrez la commande RACADM suivante :

- Avec la commande **config** : `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Avec la commande **set** : `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

Dans ce cas, aucun certificat d'autorité de certification ne doit être téléversé.

Pour désactiver la validation de certificat au cours de la négociation SSL (facultatif) :

- Avec la commande **config** : `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Avec la commande **set** : `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

Dans ce cas, vous devez téléverser le certificat d'autorité de certification en utilisant la commande RACADM suivante :

```
racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>
```

REMARQUE : Si la validation de certificat est activée, définissez les adresses de serveur de contrôleur de domaine et le nom de domaine complet qualifié du catalogue global. Vérifiez que le DNS est configuré correctement dans **Présentation → Paramètres iDRAC → Réseau**.

L'utilisation de la commande RACADM suivante peut être facultative.

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

2. Si DHCP est activé sur iDRAC7 et que vous voulez utiliser le DNS fourni par le serveur DHCP, entrez les commandes RACADM suivantes :

   - Avec la commande **config** : `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
   - Avec la commande **set** : `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. Si le protocole DHCP est désactivé sur iDRAC7 ou que vous voulez entrer manuellement l'adresse IP DNS, entrez les commandes RACADM suivantes :

   - Avec la commande **config** :

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
     config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP du DNS primaire>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP du DNS
     secondaire>
     ```

   - Avec la commande **set** :

     ```
     racadm set iDRAC.IPv4.DNSFromDHCP 0 racadm set
     iDRAC.IPv4.DNSFromDHCP.DNS1 <adresse IP DNS principale> racadm set
     iDRAC.IPv4.DNSFromDHCP.DNS2 <adresse IP DNS secondaire>
     ```

4. Si vous souhaitez définir une liste de domaines d'utilisateur pour n'avoir à entrer que le nom d'utilisateur lors de la connexion à l'interface Web, entrez la commande suivante :

   - Avec la commande **config** : `racadm config -g cfgUserDomain -o cfgUserDomainName <nom de domaine complet qualifié ou adresse IP du contrôleur de domaine> -i <index>`
   - Avec la commande **set** : `racadm set iDRAC.UserDomain.<index>.Name <nom de domaine complet qualifié ou adresse IP du contrôleur de domaine>`

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

Présentation d'Active Directory avec schéma étendu

Pour utiliser la solution de schéma étendu, vous devez disposer de l'extension de schéma Active Directory.

Extensions de schéma Active Directory

Les données Active Directory sont une base de données distribuée d'*attributs* et de *classes*. Le schéma Active Directory contient les règles qui déterminent le type de données pouvant être ajouté ou inclus dans la base de données. La classe Utilisateur est un exemple de *classe* stockée dans la base de données. Certains exemples d'attributs de classe peuvent inclure le nom, le prénom, le numéro de téléphone etc. de l'utilisateur. Vous pouvez étendre la base de données Active Directory en ajoutant vos propres *attributs* et *classes* uniques en fonction de vos besoins. Dell a étendu le schéma pour inclure les modifications nécessaires pour prendre en charge l'authentification et l'autorisation de la gestion à distance à l'aide d'Active Directory.

Chaque *attribut* ou *classe* ajouté à un schéma Active Directory existant doit être défini avec un ID unique. Pour gérer les ID uniques dans le secteur, Microsoft gère une base de données d'identificateurs d'objet Active Directory pour que, lorsque les entreprises ajoutent des extensions au schéma, ces extensions soient réputées uniques et n'entrent pas en conflit. Pour étendre le schéma dans Active Directory Microsoft, Dell a reçu des identificateurs d'objet uniques, des extensions de nom uniques et des ID d'attribut liés de manière unique pour les attributs et les classes ajoutés au service d'annuaire :

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

Présentation des extensions de schéma d'iDRAC7

Dell a étendu le schéma pour inclure des propriétés *Association*, *Périphériques* et *Privilège*. La propriété *Association* permet de lier des utilisateurs ou des groupes avec un groupe de privilèges à un ou plusieurs périphériques iDRAC7. Ce modèle fournit à l'administrateur une souplesse optimale sur les diverses combinaisons d'utilisateurs, de privilèges iDRAC7 et de périphériques iDRAC7 sur le réseau complexe.

Pour chaque périphérique iDRAC7 physique du réseau que vous voulez intégrer à Active Directory pour l'authentification et l'autorisation, créez au moins un objet Association et un objet Périphérique iDRAC7. Vous pouvez créer plusieurs objets Association qui peuvent être liés chacun à un nombre illimité d'utilisateurs, de groupes d'utilisateurs ou objets Périphérique iDRAC7. Les utilisateurs et les groupes d'utilisateurs iDRAC7 peuvent être membres de n'importe quel domaine de l'entreprise.

Cependant, chaque objet Association peut être lié (ou peut lier des utilisateurs, des groupes d'utilisateurs ou des objets Périphérique iDRAC7) à un seul objet Privilège. Cet exemple permet à l'administrateur de contrôler chacun des privilèges de l'utilisateur sur des périphériques iDRAC7 donnés.

L'objet Périphérique iDRAC7 est le lien au micrologiciel iDRAC7 pour interroger Active Directory pour l'authentification et l'autorisation. Lorsque iDRAC7 est ajouté au réseau, l'administrateur doit configurer iDRAC7 et ses objets Périphérique avec son nom Active Directory pour que les utilisateurs puissent exécuter l'authentification et l'autorisation avec Active Directory. En outre, l'administrateur doit ajouter iDRAC7 à au moins un objet Association pour que les utilisateurs puissent s'authentifier.

L'illustration suivante montre que l'objet Association fournit la connexion nécessaire à l'authentification et l'autorisation.

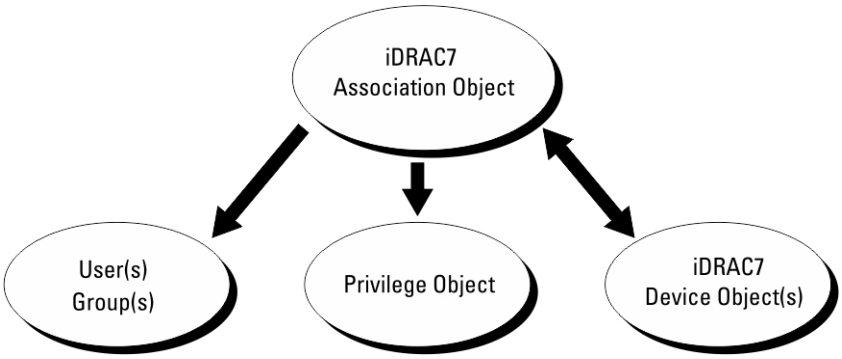

Figure 2. Configuration type pour les objets Active Directory

Vous pouvez créez un nombre illimité ou réduit d'objets Association.Cependant, vous devez créer au moins un objet Association et vous devez disposer d'un objet Périphérique iDRAC7 pour chaque périphérique iDRAC7 du réseau à intégrer à Active Directory pour l'authentification et l'autorisation avec iDRAC7.

L'objet Association permet de créer un nombre illimité ou réduit d'utilisateurs, de groupes et d'objets Périphériques iDRAC7. Toutefois, l'objet Association contient un seul objet Privilège pour chaque objet Association. L'objet Association connecte les utilisateurs ayant des privilèges sur les périphériques iDRAC7.

L'extension Dell au snap-in ADUC MMC permet d'associer l'objet Privilège et les objets iDRAC7 d'un même domaine à l'objet Association. L'extension Dell ne permet pas d'ajouter un groupe ou un objet iDRAC7 d'autres domaines comme membre de l'objet Association Object.

Lors de l'ajout de groupes universels de domaines distincts, 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 ils ne fonctionnent pas avec les groupes universels des autres domaines.

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

Accumulation de privilèges à l'aide du schéma étendu

Le mécanisme d'authentification de 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 de schéma étendu accumule les privilèges pour permettre à l'utilisateur d'utiliser le sur-ensemble de tous les privilèges affectés correspondant aux différents objets Privilège associés au même utilisateur.

L'illustration suivante montre un exemple d'accumulation de privilèges à l'aide du schéma étendu.

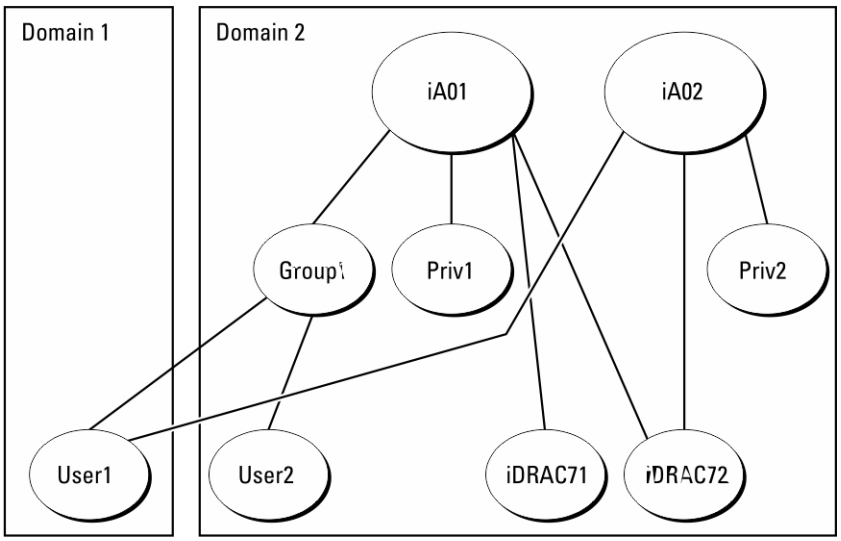

Figure 3. Accumulation de privilèges pour un utilisateur

L'illustration montre deux objets Association, A01 et A02. L'utilisateur 1 est associé à iDRAC72 via les deux objets associés.

L'authentification de 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 cet exemple, l'utilisateur 1 dispose des privilèges 1 et 2 sur iDRAC72. L'utilisateur 1 a les privilèges Priv1 sur iDRAC71 uniquement. L'utilisateur 2 a les privilèges Priv1 sur iDRAC71 et iDRAC72. En outre, cette illustration montre que l'utilisateur 1 peut se trouver dans un domaine différent et qu'il peut être membre d'un groupe.

Configuration d''Active Directory avec le schéma étendu

Pour configurer Active Directory pour qu'il accède à iDRAC7 :

1. Développez le schéma Active Directory.
2. Développez le snap-in Utilisateurs et ordinateurs Active Directory.
3. Ajoutez des utilisateurs iDRAC7 et leurs privilèges à Active Directory.
4. Configurez les propriétés Active Directory iDRAC7 à l'aide de l'interface Web ou RACADM d'iDRAC7.

Liens connexes

Présentation d'Active Directory avec schéma étendu
Installation de l'extension Dell dans le snap-in Utilisateurs et ordinateurs Microsoft Active Directory
Ajout d'utilisateurs iDRAC7 et de leurs privilèges à Active Directory
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web d'iDRAC7.
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Extension du schéma Active Directory

L'extension du schéma Active Directory schéma ajoute une unité d'organisation Dell, des classes et des attributs de schéma, des exemples de privilèges et des objets Association au schéma Active Directory. Avant d'étendre le schéma, vérifiez que vous disposez des privilèges d'administration de schéma dans le rôle de propriétaire FSMO (Flexible Single Master Operation) du contrôleur de domaine principal dans la forêt de domaines.

REMARQUE : Veillez à utiliser l'extension de schéma de ce produit s'il est différent de la génération précédente de produits RAC. Le schéma antérieur ne fonctionne pas avec ce produit.

REMARQUE : L'extension du nouveau schéma n'a pas d'impact sur les versions antérieures du produit.

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

- utilitaire Dell Schema Extender ;
- fichier script LDIF.

Si vous utilisez le fichier script LDIF, l'unité d'organisation Dell n'est 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 :

- DVDdrive:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced \LDIF_Files**
- <DVDdrive>:**\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**.

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

Utilisation de Dell Schema Extender

PRÉCAUTION : Dell Schema Extender utilise le fichier SchemaExtenderOem.ini . Pour assurer le bon fonctionnement de Dell Schema Extender, ne modifiez pas le nom de ce fichier.

1. Dans l'écran **d'accueil**, cliquez sur **Suivant**.
2. Lisez 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 **Finish** (Terminer).

   Le schéma est étendu. Pour vérifier l'extension de schéma, utilisez MMC et le snap-in de schéma Active Directory pour déterminer si les classes et les attributs Classes et attributs existent. Voir la documentation Microsoft pour plus d'informations sur MMC et le snap-in de schéma Active Directory.

Classes et attributs

Tableau 16. Définitions des 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 17. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Représente le périphérique Dell iDRAC7. iDRAC7 doit être configuré sous la forme delliDRACDevice dans Active Directory. Cette configuration permet à iDRAC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 18. delliDRACAssociationObject Class

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

Tableau 19. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Définit les privilèges (droits d'autorisation) pour iDRAC7
Type de classe	Classe auxiliaire
SuperClasses	Aucun
Attributs	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tableau 20. dellPrivileges Class

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

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Attributs	dellRAC4Privileges

Tableau 21. 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 22. 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 distinctif (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Liste des objets dellRacDevice et DelliDRACDevice qui appartiennent à ce rôle. Cet attribut est un lien suivant au lien précédent dellAssociationMembers. Numéro de lien : 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nom distinctif (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser 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
dellIsCardConfigAdmin 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
dellIsUserConfigAdmin TRUE si l'utilisateur a les droits Configuration d'utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE si l'utilisateur a les droits Effacement de journal sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.6 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si l'utilisateur a 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
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE

Nom/Description de l'attribut	OID attribué/Identifiant d'objet de syntaxe	Valeur unique
TRUE si l'utilisateur a les droits Console virtuelle sur le périphérique.	Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser 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
dellIsTestAlertUser TRUE si l'utilisateur a les droits Utilisateur pour l'alerte test sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin 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 Chaîne de non-prise en compte de la casse (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 précédent vers le lien suivant dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste des membres dellAssociationObjectMembers qui appartiennent au produit. Cet attribut est le lien précédent vers l'attribut lié dellProductMembers. Numéro de lien : 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nom distinctif (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs Active Directory pour que l'administrateur puisse gérer les périphériques iDRAC7, les utilisateurs et les groupes d'utilisateurs, les associations iDRAC7 et les privilèges iDRAC7.

Lorsque vous installez le logiciel de gestion de systèmes en utilisant le 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 l'installation. Consultez le guide d'installation rapide de Dell OpenManage pour plus d'instructions sur l'installation du logiciel de gestion de systèmes. Pour les systèmes d'exploitation Windows 64 bits, le propramme d'installation du snap-in se trouve sous :

<lecteur DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez la documentation Microsoft.

Ajout d'utilisateurs iDRAC7 et de leurs privilèges à Active Directory

En utilisant le snap-in Utilisateurs et ordinateurs Active Directory étendu Dell, vous pouvez ajouter des utilisateurs et des privilèges iDRAC7 en créant des objets Périphérique, Aassociation et Privilège. Pour ajouter chaque objet, procédez comme suit :

- Créez un objet Périphérique iDRAC7.
- Créez un objet Privilège.
- Créez un objet Association.
- Ajoutez des objets à un objet Association.

Liens connexes

Ajout d'objets à un objet Association
Création d'un objet Périphérique iDRAC7
Création d'un objet Privilège
Création d'un objet Association

Création d'un objet Périphérique iDRAC7

Pour créer un objet Périphérique iDRAC7 :

1. Dans la fenêtre **Racine de la console** MMC, cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** → **Dell Remote Management Object Advanced** (Objet avancé Dell Remote Management).
   La fenêtre **Nouvel objet** s'affiche.
3. Entrez le nom du nouvel objet. Le nom doit être identique au nom iDRAC7 que vous entrez lors de la configuration des propriétés Active Directory en utilisant l'interface Web d'iDRAC7 Web.
4. Sélectionnez **Objet Périphérique** iDRAC, puis cliquez sur OK.

Création d'un objet Privilège

Pour créer un objet Privilège :

REMARQUE : Vous devez créer un objet Privilège dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** → **Dell Remote Management Object Advanced**.
   La fenêtre **Nouvel objet** s'affiche.
3. Entrez le nom du nouvel objet.
4. Sélectionnez **Objet Privilège**, puis cliquez sur OK.
5. Cliquez avec le bouton droit de la souris sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Privilèges de gestion à distance** pour l'utilisateur ou le groupe.

Création d'un objet Association

Pour créer un objet Association :

REMARQUE : L'objet Association iDRAC7 provient d'un groupe et son étendue est Domaine local.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet de gestion à distance Dell - Avancé**.
   La fenêtre **Nouvel objet** s'affiche.
3. Entrez le nom du nouvel objet et sélectionnez **Objet Association**.

4. Sélectionnez l'étendue de l'**objet Association**, puis cliquez sur OK.
5. Fournissez des privilèges d'accès aux utilisateurs authentifiés afin de leur permettre d'accéder aux objets Association créés.

Liens connexes

Octroi de privilèges d'accès utilisateur pour les objets Association

Octroi de privilèges d'accès utilisateur pour les objets Association

Octroyez des privilèges d'accès aux utilisateurs authentifiés afin de leur permettre d'accéder aux objets Association créés.

1. Accédez à **Outils d'administration** → **Modifier ADSI**. La fenêtre **Modifier ADSI** s'affiche.
2. Dans le volet de droite, accédez à l'objet Association créé, cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
3. Dans l'onglet **Sécurité**, cliquez sur **Ajouter**.
4. Tapez `Utilisateurs authentifiés`, cliquez sur **Vérifiez les noms** et sur **OK**. Les utilisateurs authentifiés sont ajoutés à la liste des **groupes et des noms d'utilisateurs**.
5. 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 iDRAC7 ou des groupes de périphériques iDRAC7.

Vous pouvez ajouter des groupes d'utilisateurs et des périphériques iDRAC7.

Liens connexes

Ajout d'utilisateurs ou de groupes d'utilisateurs
Ajout de privilèges
Ajout de périphériques iDRAC7 ou de groupes de périphériques iDRAC7

Ajout d'utilisateurs ou de groupes d'utilisateurs

Pour ajouter des utilisateurs ou des groupes d'utilisateurs :

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

Ajout de privilèges

Pour ajouter des privilèges :

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 lors de l'authentification sur un périphérique iDRAC7. Un seul objet Privilège peut être ajouté à un objet Association.

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Entrez le nom de l'objet Privilège et cliquez sur **OK**.
3. 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 lors de l'authentification sur un périphérique iDRAC7. Un seul objet Privilège peut être ajouté à un objet Association.

Ajout de périphériques iDRAC7 ou de groupes de périphériques iDRAC7

Pour ajouter des périphériques iDRAC7 ou des groupes de périphériques iDRAC7 :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Entrez le nom des périphériques iDRAC7 ou des groupes de périphériques iDRAC7, puis cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.
4. Click sur l'onglet **Produits** pour ajouter un périphérique iDRAC7 connecté au réseau, qui est disponible pour les utilisateurs et les groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques iDRAC7 à un objet Association.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web d'iDRAC7.

Pour configurer d'Active Directory avec le schéma étendu à l'aide de l'interface Web d'iDRAC7 :

REMARQUE : Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC7*.

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Authentification des utilisateurs → Services d'annuaire → Microsoft Active Directory**.

   La page de résumé **Active Directory** apparaît.
2. Cliquez sur **Configurer Active Directory**.

   La page **Configuration et gestion d'Active Directory - Étape 1 sur 4** s'affiche.
3. Si vous le désirez, vous pouvez activer la validation de certificat et téléverser le certificat numérique signé d'autorité de certification utilisé au cours de l'initialisation des connexions SSL lors de la communication avec le serveur Active Directory (AD).
4. Cliquez sur **Suivant**.

   La page **Configuration et gestion d'Active Directory - Étape 2 sur 4** s'affiche.
5. Définissez les informations d'emplacement des serveurs et des comptes d'utilisateur Active Directory (AD), ainsi que le délai d'attente qui doit s'écouler avant qu'iDRAC7 reçoive des réponses d'AD au cours du processus d'ouverture de session.

   REMARQUE : Si la validation de certificat est activée, définissez les adresses de serveur de contrôleur de domaine et le nom de domaine complet qualifié. Vérifiez que le DNS est correctement configuré sous **Présentation générale → Paramètres iDRAC → Réseau**.
6. Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory - Étape 3 sur 4** s'affiche.
7. Sélectionnez **Schéma étendu** et cliquez sur **Suivant**.

   La page **Configuration et gestion d'Active Directory - Étape 4 sur 4** s'affiche.
8. Entrez le nom et l'emplacement de l'objet Périphérique iDRAC7 dans Active Directory (AD) et cliquez sur **Terminer**.

   Les paramètres Active Directory du mode Schéma étendu sont configurés.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Pour configurer Active Directory avec le schéma étendu en utilisant l'interface RACADM :

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

   – Avec la commande **config** :

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
   cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
   cfgADRacName <nom commun RAC> racadm config -g cfgActiveDirectory -o
   cfgADRacDomain <nom de domaine rac complet qualifié> racadm config -g
   cfgActiveDirectory -o cfgADDomainController1 <nom de domaine complet
   qualifié ou adresse IP du contrôleur de domaine> racadm config -g
   cfgActiveDirectory -o cfgADDomainController2 <nom de domaine complet
   qualifié ou adresse IP du contrôleur de domaine> racadm config -g
   cfgActiveDirectory -o cfgADDomainController3 <nom de domaine complet
   qualifié ou adresse IP du contrôleur de domaine>
   ```

   – Avec la commande **set** :

   ```
   racadm set iDRAC.ActiveDirectory.Enable 1 racadm set
   iDRAC.ActiveDirectory.Schema 2 racadm set iDRAC.ActiveDirectory.RacName
   <nom commun RAC> racadm set iDRAC.ActiveDirectory.RacDomain <nom de
   domaine rac complet qualifié> racadm set
   iDRAC.ActiveDirectory.DomainController1 <nom de domaine complet qualifié
   ou adresse IP du contrôleur de domaine> racadm set
   iDRAC.ActiveDirectory.DomainController2 <nom de domaine complet qualifié
   ou adresse IP du contrôleur de domaine> racadm set
   iDRAC.ActiveDirectory.DomainController3 <nom de domaine complet qualifié
   ou adresse IP du contrôleur de domaine>
   ```

   REMARQUE : Vous devez définir au moins une des trois adressses. iDRAC7 tente de se connecter à chacune des adresses définies l'une après l'autre jusqu'à ce qu'il établisse une connexion. Avec le schéma étendu, il s'agit du nom de domaine complet qualifié ou des adresses IP des contrôleurs de domaine où se trouve le périphérique iDRAC7.

   Pour désactiver la validation de certificat au cours de la négociation SSL (facultatif) :

   – Avec la commande **config** : `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`

   – Avec la commande **set** : `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

   REMARQUE : Dans ce cas, il n'est pas nécessaire de téléverser un certificat d'autorité de certification.

   Pour désactiver la validation de certificat au cours de la négociation SSL (facultatif) :

   – Avec la commande **config** : `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`

   – Avec la commande **set** : `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

   Dans ce cas, vous devez téléverser un certificat d'autorité de certification :

   ```
   racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>
   ```

   REMARQUE : Si la validation de certificat est activée, définissez les adresses de serveur de contrôleur de domaine et le nom de domaine complet qualifié. Vérifiez que le DNS est correctement configuré sous **Présentation → Paramètres iDRAC → Réseau**.

   L'utilisation de la commanRACADM suivante peut être facultative :

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

2. Si DHCP est activé sur iDRAC7 et que vous voulez utiliser le nom DNS fourni par le serveur DHCP, entrez la commande RACADM suivante :

   – Avec la commande **config** : `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`

   – Avec la commande **set** : `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. Si le DHCP est désactivé sur iDRAC7 ou si vous voulez entrer manuellement votre adresse IP DNS, entrez les commandes RACADM suivantes :

   – Avec de la commande **config** :

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
   config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP du DNS primaire>
   racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP du DNS
   secondaire>
   ```

   – Avec la commande **set** :

   ```
   racadm set iDRAC.IPv4.DNSFromDHCP 0 racadm set
   iDRAC.IPv4.DNSFromDHCP.DNS1 <adresse IP DNS principale> racadm set
   iDRAC.IPv4.DNSFromDHCP.DNS2 <adresse IP DNS secondaire>
   ```

4. Si vous voulez configurer une liste de domaines d'utilisateur pour n'avoir à entrer que le nom d'utilisateur lors de l'ouverture de session dans l'interface Web d'iDRAC7, entrez la commande suivante :

   – Avec la commande **config** : `racadm config -g cfgUserDomain -o cfgUserDomainName <nom de domaine complet qualifié ou adresse IP du contrôleur de domaine> -i <index>`

   – Avec la commande **set** : `racadm set iDRAC.UserDomain.<index>.Name <nom de domaine complet qualifié ou adresse IP du contrôleur de domaine>`

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

5. Appuyez sur **Entrée** pour terminer la configuration d'Active Directory avec le schéma étendu.

Test des paramètres Active Directory

Vous pouvez tester les paramètres Active Directory pour vérifier que votre configuration est correcte ou pour identifier les problèmes associés à l'échec d'une connexion Active Directory.

Test des paramètres Active Directory à l'aide de l'interface Web d'iDRAC7

Pour tester les paramètres Active Directory :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Authentification des utilisateurs → Services d'annuaire → Microsoft Active Directory**.

   La page de résumé **Active Directory** apparaît.

2. Cliquez sur **Tester les paramètres**.

3. Entrez le nom d'un utilisateur de test (par exemple, **nom_utilisateur@domaine.com**) et un mot de passe, puis cliquez sur **Démarrer le test**. Les résultats détaillés du test et le journal du test s'affichent.

   En cas d'échec d'une étape, examinez les détails dans le journal du test pour identifier le problème et une éventuelle solution.

   REMARQUE : Lorsque vous testez les paramètres Active Directory avec la validation de certificat activée, iDRAC7 impose que le serveur Active Directory soit identifié par le nom de domaine complet qualifié et non pas par une adresse IP. S'il est identifié par une adresse IP, la validation de certificat échoue, car iDRAC7 ne peut pas communiquer avec le serveur Active Directory.

Test des paramètres Active Directory en utilisant l'interface Web RACADM

Pour tester les paramètres Active Directory, utilisez la commande `testfeature`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration des utilisateurs LDAP générique

iDRC7 fournit une solution générique permettant de prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol). Cette fonction ne requiert pas d'extension de schéma dans les services d'annuaire.

Pour rendre la mise en oeuvre LDAP iDRAC7 générique, les points communs entre des services d'annuaires différents sont utilisés pour regrouper les utilisateurs et mapper ensuite la relation utilisateur-groupe. L'action de service d'annuaire est le schéma. Par exemple, ils peuvent avoir des noms d'attribut différents pour le groupe, l'utilisateur et le lien entre l'utilisateur et le groupe. Ces actions peuvent être configurées dans iDRAC7.

REMARQUE : Les connexions Authentification bifactorielle (TFA) et directe SSO (Single Sign-On) ne sont pas prises en charge pour le service d'annuaire LDAP générique.

Liens connexes

Configuration du service d'annuaire LDAP générique en utilisant l'interface Web d'iDRAC7
Configuration du service d'annuaire LDAP générique avec l'interface RACADM

Configuration du service d'annuaire LDAP générique en utilisant l'interface Web d'iDRAC7

Pour configurer le service d'annuaire LDAP générique en utilisant l'interface Web :

REMARQUE : Pour plus d'informations sur les champs, voir l'*aide en ligne d'iDRAC7*.

1. Dans l'interface Web iDRAC7, accédez à **Overview → iDRAC Settings → User Authentication → Directory Services → Generic LDAP Directory Service** (Présentation, Paramètres iDRAC, Authentification des utilisateurs, Services d'annuaire, Service d'annuaire LDAP générique).

   La page **Configuration et gestion de LDAP générique** affiche les paramètres LDAP générique actuels.
2. Cliquez sur **Configure Generic LDAP** (Configurer LDAP générique).
3. Si vous le désirez, vous pouvez activer la validation de certifiat et téléverser le certificat numériques utilisé lors de l'initialisation des connexions SSL lors de la communication avec un serveur LDAP générique.

   REMARQUE : Dans cette version, les liaisons LDAP basées sur un port non-SSL ne sont pas prises en charge. Seul LDAP over SSL est pris en charge.
4. Cliquez sur **Next** (Suivant).

   La page **Configuration et gestion LDAP génériques - Étape 2/3** s'affiche.
5. Activez l'authentification LDAP générique et définissez les iinformations d'emplacement des serveurs et des comptes d'utilisateur LDAP générique.

   REMARQUE : Si la validation de certificat est activée, définissez le nom de domaine complet qualifié du serveur LDAP et vérifiez qu'il est correctement défini sous **Présentation générale → Paramètres iDRAC → Réseau** .

   REMARQUE : Dans cette version, les groupes imbriqués ne sont pas pris en charge. Le micrologiciel recherche le membre direct du groupe pour le faire correspondre au nom de domaine d'utilisateur. En outre, un seul domaine est pris en charge. Les domaines croisés ne sont pas pris en charge.
6. Cliquez sur **Next** (Suivant).

   La page **Configuration et gestion LDAP générique - Étape 3a/3** s'affiche.

7. Cliquez sur **Groupe de rôles**.
   La page **Configuration et gestion LDAP générique - Étape 3a/3** s'affiche.
8. Définissez le nom distinct du groupe et les privilèges du groupe et cliquez sur **Appliquer**.

   REMARQUE : Si vous utilisez Novell eDirectory et que vous avez utilisé les caractères #(hachage), " (guillemets doubles), ; (point-virgule), > (supérieur à), , (virgule) ou <(inférieur à) pour le nom de domaine de groupe, vous devez utiliser le caractères d'échappement.

   Les paramètres de groupe de rôles sont enregistrés. La page **Configuration et gestion LDAP générique - Étape 3a/3** affiche les paramètres du groupe de rôles.
9. Si vous voulez configurer d'autres groupes de rôles, répétez les étapes 7 et 8.
10. Cliquez sur **Terminer**. Le service d'annuaire LDAP générique est configuré.

Configuration du service d'annuaire LDAP générique avec l'interface RACADM

Pour configurer le service d'annuaire LDAP :

- Utilisez les objets dans les groupes **cfgLdap** et **cfgLdapRoleGroup** avec la commande **config**.
- Utilisez les objets dans les groupes **iDRAC.LDAP** et **iDRAC.LDAPRole** avec la commande **set**.

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Test des paramètes du service d'annuaire LDAP

Vous pouvez tester les paramètres du service d'annuaire LDAP pour vérifier que votre configuration est correcte ou identifier les problèmes liés à l'échec d'une connexion LDAP.

Test des paramètres du service d'annuaire LDAP en utilisant l'interface Web d'iDRAC7

Pour tester les paramètres du service d'annuaire LDAP :

1. Dans l'interface iDRAC7, accédez à **Overview → iDRAC Settings → User Authentication → Directory Services → Generic LDAP Directory Service** (Présentation, Paramètres iDRAC, Authentification des utilisateurs, Services d'annuaire, Services d'annuaire LDAP générique).
   La page **Configuration et gestion de LDAP générique** affiche les paramètres LDAP générique actuels.
2. Cliquez sur **Test Settings** (Tester les paramètres).
3. Entrez le nom et le mot de passe d'un utilisateur d'annuaire choisi pour tester les paramètres LDAP. Le format dépend de l'*attribut de connexion* utilisé et le nom d'utilisateur entré doit correspondre à la valeur de l'attribut choisi.

   REMARQUE : Lors du test des paramètres LDAP avec l'option d'**activation de la validation des certificats** activée, iDRAC7 nécessite que le serveur LDAP soit identifié par le nom de domaine complet quailifé et non pas par une adresse IP. Si le serveur est identifié par une adresse IP, la validation de certificat échoue, car DRAC7 ne peut pas communiquer avec le serveur LDAP.

   REMARQUE : Lorsque LDAP générique est activé, iDRAC7 tente d'abord de connecter l'utilisateur comme utilisateur d'annuaire. S'il échoue, la recherche d'utilisateur local est activée.

   Les résultats du test et le journal du test s'affichent.

Test des paramètres du service d'annuaire LDAP en utilisant l'interface l'interface RACADM

Pour tester les paramètres du service d'annuaire LDAP, utilisez la commande `testfeature`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

8

Configuration d'ouverture de session dans d'iDRAC7 par connexion directe ou une carte à puce

Cette section fournit des informations sur la configuration d'iDRAC7 pour la connexion à l'aide d'une carte à puce (pour les utilisateurs locaux et Active Directory) et pour la connexion directe (SSO) (pour les utilisateurs Active Directory.) La connexion directe et la connexion avec une carte à puce sont des fonctions disponibles sous licence.

iDRAC7 pend en charge l'authentification Active Directory basée sur Kerberos pour pendre en charge la connexion directe et la connexion avec une carte à puce. Pour plus d'informations sur Kerberos, voir le site Web de Microsoft.

Liens connexes

Configuration d'ouverture de session par connexion directe (SSO) iDRAC7 pour les utilisateurs Active Directory
Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs locaux
Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs Active Directory

Conditions d'ouverture de session par connexion directe ou carte à puce Active Directory

Les conditions de la connexion directe ou de la connexion avec une carte à puce sont les suivantes :

- Synchronisez l'heure iDRAC7 avec l'heure du contrôleur de domaine Active Directory. Si vous ne le faites pas, l'authentification kerberos sur iDRAC7 échoue. Vous pouvez utiliser le fuseau horaire et la fonction NTP pour synchroniser l'heure. Pour ce faire, voir Configuration du fuseau horaire et du protocole NTP.
- Enregistrez iDRAC7 comme un ordinateur dans le domaine racine Active Directory.
- Générez un fichier keytab en utilisant l'outil ktpass.
- Pour activer la connexion directe pour le schéma étendu, vérifiez que l'option **Faire confiance à cet utilisateur pour la délégation à n'importe quel service** est sélectionnée dans l'onglet de **délégation** de l'utilisateur keytab. Cet onglet est disponible uniquement après avoir créé le fichier keytab en utilisant l'utilitaire ktpass.
- Configurez le navigateur pour activer la connexion SSO.
- Créez les objets Active Directory et fournissez les privilèges nécessaires.
- Pour la connexion directe, configurez la zone de recherche inverse sur les serveurs DNS du sous-réseau où se trouve iDRAC7.

  REMARQUE : Si le nom d'hôte ne correspond pas à la recherche DNS inverse, l'authentification Kerberos échoue.

Liens connexes

Définition des paramètres du navigateur afin d'activer la connexion directe (SSO) Active Directory
Enregistrement d'iDRAC7 comme ordinateur dans un domaine racine Active Directory
Génération d'un fichier Keytab Kerberos
Création d'objets Active Directory et fourniture de privilèges

Enregistrement d'iDRAC7 comme ordinateur dans un domaine racine Active Directory

Pour enregistrer iDRAC7 dans un domaine racine Active Directory :

1. Cliquez sur **Présentation générale** → **Paramètres iDRAC** → **Réseau** → **Réseau**.
   La page **Réseau** s'affiche.
2. Entrez une adresse IP de **serveur DNS préféré/secondaire**. Cette valeur est une adresse IP de serveur DNS qui fait partie du domaine racine.
3. Sélectionnez **Enregistrer iDRAC auprès du DNS.**
4. Spécifiez un **nom de domaine DNS**.
5. Vérifiez que la configuration DNS du réseau correspond aux informations DNS d'Active Directory.
   Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.

Génération d'un fichier Keytab Kerberos

Pour prendre en charge l'authentification d'ouverture de session par connexion directe et avec une carte à puce, iDRAC7 prend en charge la configuration pour s'activer comme service « kerberisé » sur un réseau Windows Kerberos. La configuration Kerberos sur iDRAC7 implique les mêmes étapes que la configuration d'un service Kerberos non–Windows Server comme principal de sécurité dans Windows Server Active Directory.

L'outil *ktpass* (fourni par Microsoft sur le CD/DVD d'installation du serveur) permet de créer les liaisons SPN (Service Principal Name) à un compte d'utilisateur et d'exporter les données d'approbation vers un fichier *keytab* Kerberos de type MIT qui établit une relation de confiance entre un utilisateur ou un système externe et le centre de distribution de clés (KDC). Le fichier keytab contient une clé cryptographique qui permet de crypter les informations entre le serveur et le centre KDC. L'outil ktpass permet aux services UNIX, qui prennent en charge l'authentification Kerberos, d'utiliser les fonctions d'interopérabilité fournies par un service KDC Kerberos Windows Server. Pour plus d'informations sur l'utilitaire **ktpass**, voir le site Web Microsoft à l'adresse **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

Avant de générer un fichier keytab, vous devez créer un compte d'utilisateur Active Directory à utiliser avec l'option **-mapuser** de la commande `ktpass`. En outre, vous devez avoir le même nom que le nom DNS iDRAC7 vers lequel vous téléversez le fichier keytab généré.

Pour générer un fichier keytab à l'aide de l'outil ktpass :

1. Exécutez l'utilitaire *ktpass* sur le contrôleur de domaine (serveur Active Directory) sur lequel vous souhaitez mapper CMC iDRAC7 à un compte utilisateur dans Active Directory.
2. Utilisez la commande ktpass suivante pour créer le fichier keytab Kerberos :

   ```
   C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -
   mapuser DOMAINNAME\username -mapOp set -crypto AES256-SHA1 -ptype
   KRB5_NT_PRINCIPAL -pass [password] -out c:\krbkeytab
   ```

   Le type de cryptage est AES256-SHA1. Le type de principal est KRB5_NT_PRINCIPAL. Utiliser les types de cryptage AES 256 pour ce compte doit être activée dans les propriétés du compte d'utilisateur auquel le nom de principal de service est associé.

   REMARQUE : Utilisez des minuscules pour le **Nom iDRAC7** et le **Nom principal de service**. Utilisez des majuscules pour le nom de domaine, comme indiqué dans l'exemple.

3. Exécutez la commande suivante :

   ```
   C:\>setspn -a HTTP/iDRAC7name.domainname.com username
   ```

   Un fichier keytab est généré.

   REMARQUE : En cas de problème avec l'utilisateur iDRAC7 pour lequel le fichier keytab est créé, créez un nouvel utilisateur et un nouveau fichier keytab. Si vous exécutez de nouveau le fichier créé initialement, il ne se configure pas correctement.

Création d'objets Active Directory et fourniture de privilèges

Procédez comme suit pour la connexion directe avec un schéma étendu Active Directory :

1. Créez l'objet Périphérique, l'objet Privilège et l'objet Association sur le serveur Active Directory.
2. Définissez des privilèges d'accès à l'objet Privilège créé. Il est recommandé de ne pas fournir les privilèges d'administrateur afin qu'aucune vérification de sécurité ne soit ignorée.
3. Associez l'objet Périphérique et l'objet Privilègeà l'aide de l'objet Association.
4. Ajoutez l'utilisateur SSO précédent (utilisateur de connexion) à l'objet Périphérique.
5. Fournissez un privilège d'accès aux *utilisateurs authentifiés* afin de leur permettre d'accéder à l'objet Association créé.

Liens connexes

Ajout d'utilisateurs iDRAC7 et de leurs privilèges à Active Directory

Définition des paramètres du navigateur afin d'activer la connexion directe (SSO) Active Directory

Cette section fournit les paramètres des navigateurs Internet Explorer et Firefox permettant d'activer la connexion directe Active Directory.

REMARQUE : Google Chrome et Safari ne prennent pas en charge Active Directory pour la connexion SSO.

Configuration d'Internet Explorer pour activer la connexion directe (SSO) Active Directory

Pour configurer les paramètres du navigateur pour Internet Explorer :

1. Dans Internet Explorer, accédez à **Intranet local** et cliquez sur **Sites**.
2. Sélectionnez les options suivantes uniquement :
   - Inclure tous les sites locaux (Intranet) non mentionnés dans d'autres zones.
   - Inclure tous les sites qui n'utilisent pas de serveur proxy.
3. Cliquez sur **Avancé**.
4. Ajoutez tous les noms de domaine relatifs qui seront utilisés pour les instances iDRAC faisant partie de la configuration de connection directe (SSO) (par exemple, **monhôte.exemple.com**.)
5. Cliquez sur **Fermer**, puis sur **OK**.

Configuration de Firefox pour activer la connexion directe (SSO) Active Directory

Pour configurer les paramètres du navigateur pour Firefox :

1. Dans la barre d'adresses, entrez `about:config`.
2. Dans **Filtre**, entrez `network.negotiate`.
3. Ajoutez le nom iDRAC7 à network.negotiate-auth.trusted-uris (en utilisant une liste d'éléments séparés par une virgule).

4. Ajoutez le nom iDRAC7 à network.negotiate-auth.trusted-uris (en utilisant une liste d'éléments séparés par une virgule).

Configuration d'ouverture de session par connexion directe (SSO) iDRAC7 pour les utilisateurs Active Directory

Avant de configurer l'ouverture de session par connexion directe iDRAC7 pour Active Directory, veillez à exécuter toutes les tâches préalables requises.

Vous pouvez configurer iDRAC7 pour une connexion directe Active Directory lorsque vous définissez un compte d'utilisateur basé sur Active Directory.

Liens connexes

Conditions d'ouverture de session par connexion directe ou carte à puce Active Directory
Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC7
Configuration d'Active Directory avec le schéma standard à l'aide de l'interface RACADM
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web d'iDRAC7.
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Configuration d'ouverture de session par connexion directe iDRAC7 pour les utilisateurs Active Directory en utilisant l'interface Web

Pour configurer l'ouverture de session par connexion directe iDRAC7 pour Active Directory :

REMARQUE : Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.

1. Déterminez si le nom DNS iDRAC7 correspond au nom de domaine complet qualifié iDRAC7. Pour ce faire, dans l'interface Web iDRAC, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau** → **Réseau** et vérifiez la propriété du **nom de domaine DNS**.
2. Lors de la configuration d'Active Directory pour définir un compte d'utilisateur basé sur le schéma standard ou étendu, exécutez les deux opérations supplémentaires suivantes pour configurer la connexion directe :
   - Téléversez le fichier keytab sur la page **Gestion et configuration Active Directory - étape 1 sur 4**.
   - Sélectionnez l'option **Activer la connexion directe** dans la page **Gestion et configuration Active Directory - Étape 2 sur 4**.

Configuration d'ouverture de session dans iDRAC7 par connexion directe pour les utilisateurs Active Directory à l'aide de l'interface RACADM

Outre les étapes exécutées lors de la configuration d'Active Directory, pour activer la connexion directe, exécutez la commande suivante :

- Avec la commande **config** :
  ```
  racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
  ```
- Avec la commande **set** :
  ```
  racadm set iDRAC.ActiveDirectory.SSOEnable 1
  ```

Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs locaux

Pour configurer un utilisateur local iDRAC7 pour la connexion par carte à puce :

1. Téléversez le certificat d'utilisateur de carte à puce et le certificat CA autorisé vers iDRAC7.
2. Activez l'ouverture de session par carte à puce

Liens connexes

Obtention de certificats
Téléversement du certificat d'utilisateur de carte à puce
Activation ou désactivation da l'ouverture de session par carte à puce

Téléversement du certificat d'utilisateur de carte à puce

Avant de téléverser le certificat d'utilisateur, veillez à exporter au format Base64 le certificat du fournisseur de la carte à puce. Les certificats SHA-2 sont également pris en charge.

Liens connexes

Obtention de certificats

Téléversement d'un certificat d'utilisateur de carte à puce en utilisant l'interface Web

Pour téléverser un certificat d'utilisateur de carte à puce :

1. Dans l'interface d'iDRAC7, accédez à **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users** (Présentation, Paramètres iDRAC, Réseau, Authentification des utilisateurs, Utilisateurs locaux).
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Smart Card Configurations** (Configurations de cartes à puce), sélectionnez **Upload User Certificate** (Téléverser un certificat d'utilisateur) et cliquez sur **Suivant**.
   La page **User Certificate Upload** (Téléversement d'un certificat d'utilisateur) s'affiche.
4. Accédez au certificat d'utilisateur en base 64, sélectionnez-le et cliquez sur **Appliquer**.

Téléversement d'un certificat d'utilisateur de carte à puce en utilisant l'interface RACADM

Pour téléverser un certificat d'utilisateur de carte à puce, utilisez l'objet **usercertupload**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et CMC) disponible à l'adresse **dell.com/support/manuals**.

Téléversement d'un certificat d'autorité de certification pour une carte à puce

Avant de téléverser le certificat d'autorité de certification, vérifiez que vous disposez d'un certificat autosigné d'autorité de certification.

Liens connexes

Obtention de certificats

Téléversement d'un certificat d'autorité de certification de confiance pour une carte à puce en utilisant l'interface Web

Pour téléverser un certificat d'autorité de certification de confiance pour une connexion avec une carte à puce :

1. Dans l'interface Web d'iDRAC7, accédez à **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users** (Présentation générale, Paramètres d'iDRAC, Authentification des utilisateurs, Utilisateurs locaux).

   La page **Utilisateurs** s'affiche.

2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.

   La page **Menu principal utilisateur** s'affiche.

3. Sous **Smart Card Configurations** (Configurations de cartes à puces), sélectionnez **Upload Trusted CA Certificate** (Téléverser un certificat d'autorité de certification de confiance) et cliquez sur **Suivant**.

   La page **Trusted CA Certificate Upload** (Téléversement d'un certificat d'autorité de certification de confiance) s'affiche.

4. Sélectionnez le certificat d'autorité de certification de confiance et cliquez sur **Appliquer**.

Téléversement d'un certificat d'autorité de certification de confiance en utilisant l'interface RACADM

Pour téléverser un certificat d'autorité de certification de confiance pour l'ouverture de session par carte à puce, utilisez l'objet **usercertupload**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs Active Directory

Avant de configurer l'ouverture de session dans iDRAC7 par carte à puce, veillez à exécuter préalablement les tâches requises.

Pour configurer l'ouverture de session iDRAC7 par carte à puce :

1. Dans l'interface Web iDRAC7, lors de la configuration d'Active Directory pour définir un compte d'utilisateur basé sur le schéma standard ou étendu, dans la page de **Gestion et de configuration d'Active Directory - étape 1 sur 4** :
   - Activez la validation de certificat.
   - Téléversez un certificat signé CA de confiance.
   - Pour téléverser le fichier keytab :
2. Activez l'ouverture de session par carte à puce. Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.

Liens connexes

Activation ou désactivation da l'ouverture de session par carte à puce
Obtention de certificats
Génération d'un fichier Keytab Kerberos
Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC7
Configuration d'Active Directory avec le schéma standard à l'aide de l'interface RACADM
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web d'iDRAC7.
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Activation ou désactivation da l'ouverture de session par carte à puce

Avant d'activer ou désactiver l'ouverture de session par carte à puce, vérifiez que :

- Vous disposez des autorisations de configuration iDRAC7.
- La configuration d'utilisateur local iDRAC7 ou Active Directory avec les certificats appropriés est terminée.

REMARQUE : Si l'ouverture de session par carte à puce est activée, SSH, Telnet, IPMI sur le LAN, Serial over LAN (Série sur LAN) et l'interface distante RACADM sont désactivés. Notez de nouveau que si vous désactivez l'ouverture de session par carte à puce, les interfaces ne sont pas activées automatiquement.

Liens connexes

Obtention de certificats

Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs Active Directory

Configuration d'ouverture de session dans iDRAC7 par carte à puce pour les utilisateurs locaux

Activation ou désactivation de l'ouverture de session carte à puce en utilisant l'interface Web

Pour activer ou désactiver la fonction d'ouverture de session par carte à puce :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Paramètres iDRAC → Authentification des utilisateurs → Carte à puce** .

   La page **Carte à puce** s'affiche.
2. Dans le menu déroulant **Configurer la connexion par carte à puce**, sélectionnez **Activé** pour activer l'ouverture de session par carte à puce ou **Activé avec l'interface RACADM distante**. Autrement, sélectionnez **Désactivé**.

   Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer** pour appliquer les paramètres.

   Un message demande un nom de connexion par carte à puce au cours des tentatives de connexion suivantes à l'aide de l'interface Web d'iDRAC7.

Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de l'interface RACADM

Pour activer l'ouverture de session par carte à puce, utilisez l'une des commandes suivantes :

- Utilisez les objets du groupe **cfgSmartCard** avec la commande **config**.
- Utilisez les objets du groupe **iDRAC.SmartCard** avec la commande **set**.

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Activation ou désactivation de l'ouverture de session par carte à puce en utilisant l'utilitaire de configuration d'iDRAC

Pour activer ou désactiver la fonction d'ouverture de session par carte à puce :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Carte à puce**.

   La page **Paramètres de carte à puce iDRAC** s'affiche.
2. Sélectionnez **Activé** pour activer la connexion par carte à puce. Autrement, sélectionnez **Désactivé**. Pour plus d'informations sur les options voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

   La fonction d'ouverture de session par carte à puce est activée ou désactivée en fonction de votre sélection.

9
Configuration d'iDRAC7 pour envoyer des alertes

Vous pouvez définir des alertes et des actions pour certains événements qui se produisent sur le système géré. Un événement se produit lorsque l'état d'un composant du système est supérieur à l'état prédéfini. Si un événement correspond à un filtre d'événement et que vous avez configuré ce filtre pour générer une alerte (e-mail, interruption SNMP, alerte IPMI, journaux du système distant ou événements WS), une alerte est envoyée à une ou plusieurs destinations définies. Si un même filtre d'événement est également configuré pour exécuter une action (redémarrage, cycle d'alimentation ou arrêt du système, par exemple), l'action est exécutée. Vous ne pouvez définir qu'une seule action pour chaque événement.

Pour configurer iDRAC7 pour qu'il envoie des alertes :

1. Activez les alertes.
2. Vous pouvez également filtrer les alertes en fonction d'une catégorie ou d'un niveau de gravité.
3. Configurez l'alerte par e-mail, l'alerte IPMI, l'interruption SNMP, le journal distant du système, le journal du système d'exploitation et/ou les paramètres d'événement WS.
4. Activez les alertes et les actions d'événements de la manière suivante :
   - Envoyez une alerte par e-mail, une alerte IPMI, des interruptions SNMP, des journaux du système distant, le journal du SE ou des événements WS aux destinations configurées.
   - Redémarrez le système géré, mettez-le hors tension ou exécutez un cycle d'alimentation sur le système géré.

Liens connexes

Activation ou désactivation des alertes
Filtrage des alertes
Définition d'alertes d'événement
Définition d'événement de récurrence d'alerte
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI
Configuration de la journalisation d'un système distant
Configuration des événements WS
ID de message d'alerte

Activation ou désactivation des alertes

Pour envoyer une alerte à des destinations définies ou exécuter une action d'événement, vous devez activer l'option d'alerte globale. Cette propriété remplace l'alerte individuelle ou les actions d'événement qui sont définies.

Liens connexes

Filtrage des alertes
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI

Activation ou désactivation des alertes en utilisant l'interface Web

Pour activer ou désactiver la génération d'alertes :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Alertes**. La page **Alertes** s'affiche.
2. Dans la section **Alertes** :
   - Sélectionnez **Activer** pour activer la génération d'alertes ou exécuter une action d'événement.
   - Sélectionnez **Désactiver** pour désactiver la génération d'alerte ou une action d'événement.
3. Cliquez sur **Appliquer** pour enregistrer le paramètre.

Activation ou désactivation des alertes en utilisant l'interface RACADM

Pour activer ou désactiver la génération d'alertes ou les actions d'événement à l'aide de la commande **config** :

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

Pour activer ou désactiver la génération d'alertes ou les actions d'événement à l'aide de la commande **config** :

```
racadm set iDRAC.IPMILan.AlertEnable 1
```

Activation ou désactivation des alertes à l'aide de l'utilitaire de configuration iDRAC

Pour activer ou désactiver la génération d'alertes ou les actions d'événement :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Alertes**.
   La page **Paramètres d'alertes iDRAC** s'affiche.
2. Dans **Événements de plate-forme**, sélectionnez **Activer** pour activer la génération d'alerte ou une action d'événement. Autrement, sélectionnez **Désactivé**. Pour plus d'informations sur les options, voir l'*Aide enligne de l'utilitaire de configuration d'iDRAC.*
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres d'alerte sont définis.

Filtrage des alertes

Vous pouvez filtrer les alertes en fonction de la catégorie et de la gravité.

Liens connexes

Activation ou désactivation des alertes
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI

Filtrage des alertes à l'aide de l'interface Web iDRAC7

Pour filtrer les alertes en fonction de la catégorie et de la gravité :

REMARQUE : Même si vous disposez de privilèges d'écriture uniquement, vous pouvez filtrer les alertes.

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Alertes**. La page **Alertes** s'affiche.
2. Dans la section **Filtre d'alertes** sélectionnez une ou plusieurs des catégories suivantes :
   - Intégrité du système
   - Entreposage
   - Configuration
   - Audit
   - Mises à jour
   - Notes de travail
3. Sélectionnez un ou plusieurs des niveaux de gravité suivants :
   - Informatif
   - Avertissement
   - Critique
4. Cliquez sur **Appliquer**.
   La section **Résultats des alertes** affiche les résultats en fonction de la catégorie et de la gravité sélectionnées.

Filtrage des alertes à l'aide de l'interface RACADM

Pour filtrer les alertes, utilisez la commande **eventfilters**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Définition d'alertes d'événement

Vous pouvez définir des alertes d'événements, telles que les alertes par e-mail, les alertes IPMI, les interruptions SNMP, les journaux système distants, les journaux du système d'exploitation et les événements WS à envoyer aux destinations configurées.

Liens connexes

Activation ou désactivation des alertes
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI
Filtrage des alertes
Configuration de la journalisation d'un système distant
Configuration des événements WS

Définition d'alertes d'événements dans l'interface Web

Pour définir une alerte d'événement dans l'interface Web :

1. Assurez-vous que vous avez configuré l'alerte par e-mail, l'alerte IPMI, les paramètres d'interruptions SNMP et/ou les paramètres du journal système distant.
2. Allez sur **Présentation** → **Serveur** → **Alertes**.
   La page **Alertes** s'affiche.

3. Sous **Résultats d'alertes**, sélectionnez une alerte ou toutes les alertes suivantes des événements appropriés :
   - Alerte par e-mail
   - Interruption SNMP
   - Alerte IPMI
   - Journal système distant
   - Journal du SE
   - Événements WS
4. Cliquez sur **Appliquer**.
   Le paramétrage est enregistré.
5. Dans la section **Alertes**, sélectionnez **Activer** pour envoyer des alertes aux destinations définies.
6. Facultativement, vous pouvez envoyer un événement test. Dans le champ **ID de message pour tester l'événement**, saisissez l'ID de message pour tester si l'alerte est générée, puis cliquez sur **Tester**. Pour la liste des ID de message, voir le *Guide des messages d'événements* disponible à l'adresse **dell.com/support/manuals**.

Définition d'alertes d'événement à l'aide de l'interface RACADM

Pour définir une alerte d'événement, utilisez la commande **eventfilters**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Définition d'événement de récurrence d'alerte

Vous pouvez configurer iDRAC pour générer des événements supplémentaires à des intervalles spécifiques, si le système continue de fonctionner à une température qui est supérieure à la limite du seuil de température d'entrée. L'intervalle par défaut est de 30 jours. La plage valide va de 0 à 365 jours. Une valeur égale à '0 'indique que l'événement de récurrence est désactivé.

REMARQUE : Vous devez avoir le privilège Configurer iDRAC pour définir la valeur de récurrence d'alerte.

Définition d'événements de récurrence d'alerte à l'aide de l'interface Web iDRAC7

Pour définir la valeur de récurrence d'alerte :

1. Dans l'interface Web iDRAC7, accédez à **Présentation** → **Serveur** → **Alertes** → **Récurrence d'alerte**.
   La page **Récurrence d'alerte** s'affiche.
2. Dans la colonne **Récurrence**, entrez la valeur de fréquence d'alerte pour le ou les types de gravité, alerte et catégorie requis.
   Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer**.
   Les paramètres de récurrence d'alerte sont enregistrés.

Définition d'événements de récurrence d'alerte à l'aide de l'interface RACADM

Pour définir l'événement de récurrence d'alerte à l'aide de l'interface RACADM, utilisez la sous-commande **eventfilters**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC)*.

Définition d'actions d'événement

Vous pouvez définir des actions d'événement, telles qu'un redémarrage, un cycle d'alimentation, une mise hors tension, ou n'exécuter aucune action sur le système.

Liens connexes

Filtrage des alertes

Activation ou désactivation des alertes

Définition d'actions d'événement à l'aide de l'interface Web

Pour configurer une action :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Serveur** → **Alertes** . La page **Alertes** s'affiche.
2. Sous **Résultats d'alerte**, dans le menu déroulant **Actions** de chaque événement, sélectionnez une action :
   - Redémarrer
   - Cycle d'alimentation
   - Mettre hors tension
   - Aucune action
3. Cliquez sur **Appliquer**.

   Le paramétrage est enregistré.

Définition d'actions d'événements à l'aide de l'interface RACADM

Pour configurer une action d'événement, utilisez l'une des méthodes suivantes :

- La commande **eventfilters**.
- L'objet **cfgIpmiPefAction** avec la commande **config**.

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI

La station de gestion utilise des interceptions SNMP (Simple Network Management Protocol) et IPIMI (Intelligent Platform Management Interface) pour recevoir des données d'iDRAC7. Pour les systèmes disposant de nombreux nœuds, il peut ne pas être efficace pour une station de travail d'appeler chaque iDRAC7 pour chaque événement qui peut se produire. Par exemple, les interceptions d'événements peuvent aider une station de gestion avec l'équilibrage de charge entre les nœuds ou en émettant une alerte en cas d'échec de l'authentification.

Vous pouvez configurer les destinations d'alerte IPv4 et IPv6, les paramètres e-mail et les paramètres de serveur SMTP et tester ces paramètres.

Avant de configurer les paramètres e-mail, d'interruption SNMP ou d'interruption IPMI, vérifiez que :

- Vous disposez de l'autorisation de configuration RAC.
- Vous avez défini des filtres d'événements.

Liens connexes

Configuration des destinations d'alerte IP

Configuration des paramètres d'alerte par e-mail

Configuration des destinations d'alerte IP

Vous pouvez configurer des adresses IPv6 ou IPv4 pour recevoir les alertes IPMI ou les interruptions SNMP.

Configuration de destinations d'alerte IP en utilisant l'interface Web

Pour configurer les paramètres des destinations d'alerte à l'aide de l'interface Web :

1. Allez sous **Présentation** → **Serveur** → **Alertes** → **Paramètres SNMP et d'e-mail**.
2. Sélectionnez l'option **État** pour activer une destination d'alerte (adresse IPv4, adresse IPv6, ou Nom de domaine complet (FQDN)) pour recevoir les interruptions.

   Vous pouvez spécifier jusqu'à huit adresses de destination. Pour en savoir plus sur les options, voir l'*aide en ligne iDRAC7*.
3. Entrez la chaîne de communauté SNMP de l'iDRAC7 et le numéro de port de l'alerte SNMP.

   Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.

   REMARQUE : La valeur de chaîne de communauté indique la chaîne de communauté à utiliser dans une alerte SNMP (Simple Network Management Protocol) envoyée par iDRAC7. Veillez à ce que la chaîne de communauté de destination soit identique à la chaîne de communauté iDRAC7. La valeur par défaut est Publique.
4. Pour déterminer si l'adresse IP reçoit les interruptions IPMI ou SNMP, cliquez sur **Envoyer** sous **Tester les interruptions IMPI** et **Tester les interruptions SNMP** respectivement.
5. Cliquez sur **Appliquer**.

   Les destinations d'alerte sont configurées.
6. Dans la section **Format des interruptions SNMP**, sélectionnez la version du protocole à utiliser pour l'envoi des interruptions aux destinations d'interruption (**SNMP v1** ou **SNMP v2**) puis cliquez sur **Appliquer**.

   REMARQUE : L'option **Format des interruptions SNMP** s'applique uniquement aux interruptions SNMP, et non aux interruptions IPMI. Les interruptions IPMI sont toujours envoyées au format SNMP v1 et ne sont pas basées sur l'option **Format des interruptions SNMP** configurée.

   Le format des interruptions SNMP est configuré.

Configuration des destinations d'alerte IP en utilisant l'interface RACADM

Pour définir les paramètres d'alerte d'interruption :

1. Pour activer les interruptions :
   - Pour une adresse IPv4 :
     ```
     racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i (index) (0|1)
     ```
   - Pour une adresse IPv6 :
     ```
     racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i (index)
     (0|1)
     ```
     , où (index) est l'index de destination et 0 ou 1 désactive ou active l'interruption.

     Par exemple, pour activer l'interruption avec l'index 4, entrez la commande suivante :
     ```
     racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
     ```
2. Pour définir l'adresse de destination de l'interruption :
   ```
   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i [index]
   [adresse IP]
   ```
   où <[index]> est l'index de destination de l'interruption et <[adresse IP]>, l'adresse IP de destination du système qui reçoit les alertes d'événement de plate-forme.
3. Configurez la chaîne de nom de communauté SNMP :
   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [nom]
   ```
   où <[nom]> est le nom de communauté SNMP.
4. Pour tester l'interruption, si nécessaire :
   ```
   racadm testtrap -i [index]
   ```
   , où <[index]> est l'index de destination de l'interruption à tester.

   Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration des adresses de destination d'alerte IP à l'aide de l'utilitaire de configuration d'iDRAC

Vous pouvez configurer les destinations d'alerte (IPv4, IPv6, ou FQDN) à l'aide de l'utilitaire Paramètres iDRAC. Pour ce faire :

1. Dans l'**utilitaire de configuration d'iDRAC**, accédez à **Alertes**.

   La page **Paramètres d'alerte d'iDRAC** s'affiche.
2. Sous **Paramètres d'interruption**, activez la ou les adresses IP pour recevoir les interruptions et entrez la ou les adresses IPv4, IPv6, ou FQDN de destination. Vous pouvez définir jusqu'à huit adresses.
3. Entrez le nom de la chaîne de communauté.

   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
4. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

   Les destinations d'alerte sont configurées.

Configuration des paramètres d'alerte par e-mail

Vous pouvez configurer l'adresse e-mail destinataire des alertes par e-mail. Configurez également les paramètres d'adresse du serveur SMTP.

REMARQUE : Si vous utilisez le serveur de messagerie Microsoft Exchange Server 2007, veillez à ce que le nom de domaine d'iDRAC soit configuré pour que le serveur de messagerie puisse recevoir les alertes par e-mail d'iDRAC.

REMARQUE : Les alertes par e-mail prennent en charge les adresses iPv4 et IPv6. Le nom de domaine DNS DRAC doit être défini lorsque vous utilisez IPv6.

Liens connexes

Configuration des paramètres de l'adresse du serveur de messagerie SMTP

Configuration des paramètres des alertes par e-mail à l'aide de l'interface Web :

Pour configurer les paramètres d'alerte par e-mail en utilisant l'interface Web :

1. Allez sous **Présentation** → **Serveur** → **Alertes** → **Paramètres SNMP et e-mail**.
2. Sélectionnez l'option **État** pour activer l'adresse e-mail pour recevoir des alertes et tapez une adresse e-mail valide. Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC7.*
3. Cliquez sur **Envoyer** sous **E-mail test** pour tester les paramètres des alertes par e-mail.
4. Cliquez sur **Appliquer**.

Configuration des paramètres des alertes par e-mail à l'aide de RACADM

Pour configurer les paramètres des alertes par e-mail :

1. Pour activer les alertes par e-mail :
   - Utilisation de la commande **config** :
     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [index] [0|1]
     ```
     où `[index]` est l'index de destination de l'e-mail. 0 désactive l'alerte par e-mail et 1 active l'alerte.
     L'index de destination de l'e-mail peut être une valeur comprise entre 1 et 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
     ```
   - Avec la commande **set** :
     ```
     racadm set iDRAC.EmailAlert.Enable.[index] 1
     ```
     où `[index]` est l'index de destination de l'e-mail. 0 désactive l'alerte par e-mail et 1 active l'alerte.
     L'index de destination de l'e-mail peut être une valeur comprise entre 1 et 4. Par exemple, pour activer l'e-mail avec l'index 4, entrez la commande suivante :
     ```
     racadm set iDRAC.EmailAlert.Enable.4 1
     ```
2. Pour configurer les paramètres de l'e-mail :
   - Avec la commande **config** :
     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 [adresse e-mail]
     ```
     où 1 est l'index de destination de l'e-mail et `[email-address]` est l'adresse e-mail de destination qui reçoit les alertes d'événements de la plate-forme.
   - Avec la commande **set** :
     ```
     racadm set iDRAC.EmailAlert.Address.1 [email-address]
     ```
     où 1 est l'index de destination de l'e-mail et `[email-address]` est l'adresse e-mail de destination qui reçoit les alertes d'événements de la plate-forme.

3. Pour configurer un message personnalisé :
   - Avec la commande **config** :
     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i [index]
     [message personnalisé]
     ```
     où `[index]` est l'index de destination de l'e-mail et `[custom-message]`, le message personnalisé.
   - Avec la commande **set** :
     ```
     racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
     ```
     où `[index]` est l'index de destination de l'e-mail et `[custom-message]`, le message personnalisé.
4. Pour tester l'alerte par e-mail configurée, si nécessaire :
   ```
   racadm testemail -i [index]
   ```
   , où `[index]` est l'index de destination dl'email à tester.

   Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration des paramètres de l'adresse du serveur de messagerie SMTP

Vous devez configurer l'adresse du serveur SMTP pour que les alertes par e-mail soient envoyées à des destinations spécifiées.

Définition des paramètres d'adresse du server de messagerie SMTP en utilisant l'interface Web iDRAC7

Pour définir l'adresse du serveur SMTP :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale → Serveur → Alertes → Paramètres SNMP et de messagerie**.
2. Entrez l'adresse IP valide ou le nom de domaine pleinement qualifié (FQDN) du serveur SMTP à utiliser au cours de la configuration.
3. Sélectionnez l'option **Activer l'authentification**, puis entrez le nom d'utilisateur et le mot de passe d'un utilisateur qui a accès au serveur SMTP.
4. Entrez le numéro de port SMTP.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC7*.
5. Cliquez sur **Appliquer**.

   Les paramètres SMTP sont définis.

Définition des paramètres d'adresse du serveur de messagerie SMTP à l'aide de l'interface RACADM

Pour configurer le serveur d'e-mail SMTP utilisez l'une des méthodes suivantes :

- Avec la commande **set** :
  ```
  racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <adresse IP du serveur d'e-
  mail SMTP>
  ```
- Utilisation de la commande **config** :
  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP adresse
  IP du serveur de messagerie SMTP>
  ```

Configuration des événements WS

Le protocole des événements WS est utilisé pour un service client (abonné) pour enregistrer l'intérêt (abonnement) sur un serveur (source d'événement) pour recevoir les messages contenant les événements de serveur (notifications ou messages d'événement). Les clients souhaitant recevoir des messages d'événement WS peuvent s'inscrire à iDRAC et recevoir des événements de tâche du Lifecycle Controller.

Les étapes requises pour configurer la fonction des événements WS afin de recevoir les messages d'événements WS relatifs aux tâches du Lifecycle Controller sont décrites dans le document de spécifications Web service Eventing Support for iDRAC7 1.30.30 (Prise en charge des événements Web Service pour iDRAC7 1.30.30). Outre ce document, consultez le document DSP0226 (Spécification de gestion WS DMTF), notifications de section 10 (Événements) pour des informations exhaustives concernant le protocole des événements WS. Les tâches relatives au Lifecycle Controller sont décrites dans le document DCIM Job Control Profile (Profil du contrôle des tâches DCIM).

ID de message d'alerte

Le tableau suivant répertorie les ID de message affichés pour les alertes.

Tableau 23. ID de message d'alerte

ID du message	Description
AMP	Intensité du courant
ASR	Réinitialisation auto du système
BAR	Sauvegarde/Restauration
BAT	Événement batterie
BIOS	Gestion du BIOS
BOOT	Contrôle de l'amorçage
CBL	Câble
CPU	Processeur
CPUA	Proc absent
CTL	Contrôle stockage
DH	Gestion cert
DIS	Découverte automatique
ENC	Enceinte stockage
FAN	Événement ventilateur
FSD	Débogage
HWC	Configuration matérielle
IPA	Changement d'adresse IP DRAC
ITR	intrusion
JCP	Contrôle des tâches
LC	Lifecycle Contr
LIC	Licence
LNK	État de la liaison
LOG	Événement journal
MEM	Mémoire
NDR	Pilote SE NIC
Carte réseau	Configuration NIC
OSD	Déploiement du SE
OSE	Événement OS

ID du message	Description
PCI	Périphérique PCI
PDR	Disque physique
PR	Changement composant
PST	BIOS POST
Bloc d'alimentation	Alimentation électrique
PSUA	Unité d'alimentation absente
PWR	Utilisation de l'énergie
RAC	Événement RAC
RDU	Redondance
RED	Téléchargement FW
RFL	Média IDSDM
RFLA	IDSDM Absent
RFM	SD FlexAddress
RRDU	Redondance IDSDM
RSI	Service à distance
SEC	Événement sécurité
SEL	Journal des événements système
SRD	RAID logiciel
SSD	PCIe SSD
STOR	Stockage
SUP	Tâche de mise à jour FW
SWC	Configuration logicielle
SWU	Changement logiciel
SYS	Infos système
TMP	Température
TST	Alerte test
UEFI	Événement UEFI
USR	Suivi utilisateur
VDR	Disque virtuel
VF	Carte SD vFlash
VFL	Événement vFlash
VFLA	vFlash absent
VLT	Tension
VME	Média virtuel
VRM	Console virtuelle
WRK	Note de travail

10

Gestion des journaux

iDRAC7 fournit un journal Lifecycle qui contient les événements liés au système, aux périphériques de stockage, aux périphériques de réseau, aux mises à jour de micrologiciel, aux modifications de configuration, aux messages de licence, etc. Cependant, les événements du système sont également disponibles comme journal distinct appelé SEL (System Event Log). Le journal Lifecycle est accessible via l'interface Web iDRAC7, l'interface RACADM et l'interface WS-MAN.

Lorsque la taille du journal Lifecycle atteint 800 Ko, les journaux sont compressés et archivés. Vous pouvez afficher uniquement les entrées de journal non archivées et appliquer des filtres et des commentaires aux journaux non archivés. Pour afficher les journaux archivés, vous devez exporter l'ensemble du journal Lifecycle vers un emplacement sur votre système.

Liens connexes

- Affichage du journal des événements système
- Affichage du journal Lifecycle
- Ajout de notes de travail
- Configuration de la journalisation d'un système distant

Affichage du journal des événements système

Lorsqu'un événement se produit sur un système géré, il est enregistré dans le journal SEL (System Event Log). La même entrée SEL est disponible dans le journal LC.

Affichage du journal des événements système en utilisant l'interface Web

Pour afficher le journal SEL, dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Journaux**.

La page du **journal des événements système** affiche un indicateur d'intégrité du système, un horodatage et la description de chaque événement consigné. Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.

Cliquez sur **Enregistrer sous** pour enregistrer le journal **SEL** dans le répertoire de votre choix.

REMARQUE : Si vous utilisez Internet Explorer et s'il existe un problème lors de l'enregistrement, téléchargez Cumulative Security Update for Internet Explorer. Vous pouvez le télécharger à partir du site Web de support de Microsoft à l'adresse **support.microsoft.com**.

Pour effacer les journaux, cliquez sur **Effacer le journal**.

REMARQUE : Le bouton **Effacer le journal** n'apparaît que si vous disposez de l'autorisation Effacer les journaux.

Une fois que le journal SEL est effacé, une entrée est consignée dans le journal du Lifecycle Controller. L'entrée de journal inclut le nom d'utilisateur et l'adresse IP de l'emplacement où le journal SEL a été effacé.

Affichage du journal des événements système à l'aide de l'interface RACADM

Pour afficher le journal SEL :

```
racadm getsel <options>
```

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

Pour afficher le nombre d'entrées du journal SEL : `racadm getsel -i`

Pour effacer les entrées du journal SEL : `racadm clrsel`

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Affichage du journal des événements système à l'aide de l'utilitaire Paramètres iDRAC

Vous pouvez afficher le nombre total d'enregistrements dans le journal des événements système (SEL) et les effacer à l'aide de l'utilitaire Paramètres iDRAC. Pour ce faire :

1. Depuis l'utilitaire Paramètres iDRAC, allez sous **Journal des événements système**.
   La page **Paramètres iDRAC.Journal des événements système** affiche le **Nombre total d'enregistrements**.
2. Pour effacer les enregistrements, sélectionnez **Oui**. Sinon, sélectionnez **Non**.
3. Pour afficher les événements système, cliquez sur **Affichage du journal d'événements du système**.
4. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

Affichage du journal Lifecycle

Les journaux Lifecycle Controller contiennent l'historique des modifications associées aux composants installés sur un système géré. Les journaux disponibles contiennent des événements sur :

- Périphériques de stockage
- Système
- Périphériques réseau
- Configuration
- Audit
- Mises à jour
- Notes de travail

Lorsque vous vous connectez ou vous déconnectez de l'iDRAC7 à l'aide de l'une des interfaces suivantes, les événements d'ouverture, de fermeture de session ou d'échec d'ouverture sont consignés dans les journaux Lifecycle :

- Telnet
- SSH
- Interface Web
- RACADM
- SM-CLP
- IPMI sur le LAN
- Série
- Console virtuelle
- Média virtuel

Vous pouvez filtrer les journaux en fonction de la catégorie et du niveau gravité et afficher, exporter et ajouter une note de travail à un événement de journal.

Liens connexes

Filtrage des journaux Lifecycle
Exportation des journaux du Lifecycle Controller via l'interface Web
Ajout de commentaire aux journaux Lifecycle

Affichage du journal Lifecycle en utilisant l'interface Web

Pour afficher les journaux Lifecycle, cliquez sur **Présentation générale** → **Serveur** → **Journaux** → **Lifecycle Log**. La page **Journal Lifecycle** s'affiche. Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.

Filtrage des journaux Lifecycle

Vous pouvez filtrer les journaux en fonction de la catégorie, de la gravité, d'un mot clé ou d'une plage de dates.

Pour filtrer les journaux Lifecycle :

1. Dans la page **Journal LIfecycle** dans la section **Filtre de journal**, exécutez l'ensemble ou une partie des opérations suivantes :
   - Sélectionnez le **Type de journal** dans la liste déroulante.
   - Sélectionnez le niveau de gravité dans la liste déroulante **Gravité**.
   - Entrez un mot clé.
   - Définissez la plage de dates.
2. Cliquez sur **Appliquer**.

   Les entrées du journal filtré s'affichent dans les **Résultats du journal**.

Ajout de commentaire aux journaux Lifecycle

Pour ajouter des commentaires aux journaux lifecycle :

1. Dans la page **Journal Lifecycle**, cliquez sur l'icône + de l'entrée de journal appropriée.

   Les détails d'ID de message s'affichent.
2. Entrez les commentaires de l'entrée de journal dans la zone **Commentaire**.

   Le commentaire s'affiche dans la zone **Commentaire**.

Affichage du journal Lifecycle à l'aide de l'interface RACADM

Pour afficher les journaux Lifecycle, utilisez la commande `lclog`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Exportation des journaux du Lifecycle Controller

Vous pouvez exporter le journal du Lifecycle Controller entier (entrées actives et archivées) dans un seul fichier compressé XML sur un partage réseau ou sur le système local. L'extension de fichier XML compacté est **.xml.gz**. Les entrées de fichier sont commandées de façon séquentielle en fonction de leurs numéros de séquence, commandées à partir du numéro de séquence le plus bas jusqu'au plus élevé.

Exportation des journaux du Lifecycle Controller via l'interface Web

Pour exporter les journaux du Lifecycle Controller à l'aide de l'interface Web :

1. Dans la page **Journal Lifecycle**, cliquez sur **Exporter** .
2. Sélectionnez l'une des options suivantes :
   - **Réseau** : exportez les journaux Lifecycle vers un emplacement partagé du réseau.
   - **Local** : exportez les journaux Lifecycle vers un emplacement sur le système local.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.

3. Cliquez sur **Exporter** pour exporter le journal sur un emplacement spécifié.

Exportation des journaux du Lifecycle Controller via la RACADM

Pour exporter les journaux du Lifecycle Controller à l'aide de la RACADM, utilisez la commande `lclog export`. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC* disponible à l'adresse **dell.com/support/manuals** ou **dell.com/esmmanuals**.

Ajout de notes de travail

Chaque utilisateur qui ouvre une session sur iDRAC7 peut ajouter des notes de travail qui sont stockées dans le journal Lifecycle sous la forme d'un événement. Vous devez disposer du privilège Journaux iDRAC7 pour pouvoir ajouter des notes de travail. Chaque note peut contenir jusqu'à 255 caractères.

REMARQUE : Vous ne pouvez pas supprimer une note de travail.

Pour ajouter une note de travail :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Serveur** → **Propriétés** → **Résumé**.
   La page du **Résumé du système** s'affiche.
2. Dans **Notes de travail**, entrez le texte dans la zone de texte vide.

   REMARQUE : Il est recommandé de ne pas utiliser un trop grand nombre de caractères spéciaux.
3. Cliquez sur **Ajouter**.
   La note de travail est ajoutée au journal. Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.

Configuration de la journalisation d'un système distant

Vous pouvez envoyer des journaux Lifecycle à un système distant. Auparavant, vérifiez que :

- Il existe une connectivité réseau entre iDRAC7 et le système distant.
- Le système distant et iDRAC7 se trouvent dans le même réseau.

Configuration de la journalisation d'un système distant à l'aide de l'interface Web

Pour configurer les paramètres d'un serveur syslog distant :

1. Dans l'interface Web iDRAC7, accédez à **Présentation** → **Serveur** → **Journaux** → **Paramètres**.
   L'écran **Paramètres du syslog distant** s'affiche.
2. Activez le serveur syslog distant, définissez l'adresse du serveur et spécifiez le numéro de port. Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer**.
   Les paramètres sont enregistrés. Tous les journaux écrits dans le journal Lifecycle sont écrits simultanément sur le ou les serveurs distants configurés.

Configuration de la journalisation du système distant en utilisant l'interface RACADM

Pour configurer les paramètres du serveur syslog distant, utilisez l'un des objets suivants :

- Objets du groupe **cfgRemoteHosts** avec la commande **config**.
- Objets du groupe **iDRAC.SysLog** avec la commande **set**.

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

11

Surveillance et gestion de l'alimentation

Vous pouvez utiliser iDRAC7 pour surveiller et gérer l'alimentation du système géré afin de protéger le système contre les surtensions en distribuant et en régulant de manière appropriée la consommation électrique du système.

Les principales fonctions sont les suivantes :

- **Surveillance de l'alimentation** : affichage de l'état de l'alimentation, historique des mesures d'alimentation, moyennes de courant, pics, etc. associés au système géré.
- **Limitation de la puissance :** affichage et définition de la limitation de puissance du système géré, y compris l'affichage de la consommation électrique potentielle maximale et minimale. Il s'agit d'une fonction disponible sous licence.
- **Contrôle de l'alimentation :** exécution à distance d'opérations de contrôle de l'alimentation (mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation et arrêt normal) sur le système géré.
- Options d'alimentation : configuration des options d'alimentation, telles que stratégie de redondance, composant de rechange à chaud et correction du facteur de puissance.

Liens connexes

Surveillance de l'alimentation
Exécution d'opérations de contrôle de l'alimentation
Limitation de l'alimentation
Configuration des options d'alimentation
Activation ou désactivation du bouton Marche/Arrêt

Surveillance de l'alimentation

iDRAC7 surveille la consommation d'énergie du système en continu et affiche les valeurs suivantes :

- Seuils d'avertissement de consommation d'énergie et critiques.
- Valeurs de puissance cumulée, de puissance de crête et pic d'intensité de courant électrique.
- Consommation d'énergie au cours de la dernière heure, du dernier jour ou de la dernière semaine.
- Consommation d'énergie moyenne, minimale et maximale
- Historique des pics et horodatage des pics.
- Pic de marge de sécurité et valeurs de marge de sécurité instantanée (pour les serveurs en rack et de type tour).

Surveillance de l'alimentation avec l'interface Web

Pour afficher les informations de surveillance de l'alimentation, dans l'interface Web iDRAC7, accédez à **Présentation générale → Serveur → Alimentation/Thermique → Surveillance de l'alimentation**. La page **Surveillance de l'alimentation** s'affiche. Pour plus d'informations voir l'*Aide en ligne d'iDRAC7*.

Surveillance de l'alimentation en utilisant l'interface RACADM

Pour afficher les informations de surveillance de l'alimentation, utilisez les objets du groupe **System.Power** avec la commande **get** ou l'objet **cfgServerPower** avec la commande **getconfig**. Pour plus d'informations, voir le *RACADM*

Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Exécution d'opérations de contrôle de l'alimentation

iDRAC7 permet d'exécuter à distance une mise sous tension, une mise hors tension, une réinitialisation, un arrêt normal, une interruption NMI (Non-Masking Interrupt) ou un cycle d'alimentation à l'aide de l'interface Web ou RACADM.

Vous pouvez également exécuter ces opérations en utilisant les services à distance Lifecycle Controller ou WS-Management. Pour plus d'informations, voir le *Lifecycle Controller Remote Services Quick Start Guide* (Guide d'utilisation des services à distance Lifecycle Controller) disponible sur **dell.com/support/manuals** et le document de profils *Dell Power State Management* (Gestion de l'état d'alimentation Dell) disponibles sur le site **delltechcenter.com**.

Exécution des opérations de contrôle de l'alimentation en utilisant l'interface Web

Pour exécuter des opérations de contrôle d'alimentation :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Alimentation/Thermique** → **Configuration de l'alimentation** → **Contrôle de l'alimentation**. La page **Contrôle de l'alimentation** s'affiche.
2. Sélectionnez l'opération d'alimentation appropriée :
   - Mettez le système sous tension
   - Mettez le système hors tension.
   - NMI (interruption non masquable)
   - Arrêt normal
   - Réinitialiser le système (démarrage à chaud)
   - Exécuter un cycle d'alimentation du système (démarrage à froid)
3. Cliquez sur **Appliquer**. Pour plus d''informations, voir l'*aide en ligne d'iDRAC7*.

Exécution d'opérations de contrôle de l'alimentation en utilisant l'interface RACADM

Pour exécuter des actions d'alimentation, utilisez la commande **serveraction**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

Limitation de l'alimentation

Vous pouvez afficher les limites de seuil de puissance qui couvrent la plage de consommation électrique CA et CC qu'un système soumis à une forte charge de travail présente au centre de données. Cette fonction est disponible sous licence.

Limitation de la puissance dans les serveurs lames

Avant la mise sous tension d'un serveur lame, iDRAC7 fournit à CMC ses besoins en puissance qui sont plus élevés que la puissance réelle que la lame peut consommer qui est calculée en fonction d'informations d'inventaire matériel limitées. Il peut demander une plage de puissances plus petite après la mise sous tension du serveur en fonction de la puissance réelle consommée par le serveur. Si la consommation électrique augmente au fil du temps et que le serveur atteint presque sa consommation électrique maximale, iDRAC7 peut demander une augmentation de la consommation électrique potentielle maximale, ce qui augmente l'enveloppe énergétique. iDRAC7 augmente uniquement sa demande de consommation électrique potentielle maximale à CMC. Il ne demande pas une puissance minimale potentielle inférieure si la consommation diminue. iDRAC7 continue de demander plus de puissance si la consommation électrique dépasse la puissance allouée par CMC.

Une fois le système sous tension et initialisé, iDRAC7 calcule une nouvelle exigence de puissance en fonction de la configuration de la lame. La lame reste sous tension, même si CMC ne parvient pas à satisfaire la nouvelle demande de puissance.

CMC récupère toute puissance non utilisée des serveurs à priorité inférieure et alloue ensuite cette puissance récupérée à un module d'infrastructure ou un serveur à priorité supérieure.

Si la puissance allouée est insuffisante, le serveur lame n'est pas mis sous tension. Si la lame reçoit une puissance suffisante,iDRAC7 le met sous tension.

Affichage et configuration d'une stratégie de limitation de puissance

Lorsqu'une stratégie appropriée de limitation de puissance est activée, elle applique les limites de puissance définies par l'utilisateur au système. Si la stratégie n'est pas activée, elle utilise la stratégie de protection de la puissance du matériel mise en œuvre par défaut. Cette stratégie de protection de puissance est indépendant de la stratégie définie par l'utilisateur. Les performances du système sont ajustées dynamiquement pour maintenir la consommation électrique proche du seuil défini.

La consommation électrique réelle peut être inférieure pour les faibles charges de travail et peut dépasser temporairement le seuil jusqu'à l'ajustement des performances. Par exemple, pour une configuration système donnée, la consommation électrique potentielle maximale est de 700 W et la consommation électrique potentielle moyenne est de 500 W. Vous pouvez définir et activer un seuil de budget énergétique pour faire passer la consommation de 650 W à 525 W. À partir de là, les performances du système sont ajustées dynamiquement pour maintenir la consommation électrique pour ne pas dépasser le seuil de 525 W défini par l'utilisateur.

Si la valeur de limitation est inférieure au seuil minimal recommandé, iDRAC7 ne peut pas maintenir la limite de puissance demandée.

Vous pouvez définir la valeur en watts, BTU/h ou sous la forme d'un pourcentage (%) de la limite de puissance maximale recommandée.

Lorsque vous définissez le seuil de limite de puissance en BTU/h, la conversion en watts est arrondie à l'entier le plus proche. Lors de la lecture du seuil de limite de puissance, la conversion des watts en BTU/h est de nouveau arrondie de cette manière. Par conséquent, la valeur écrite peut être nominalement différente de la valeur lue. Par exemple, la lecture du seuil de 600 BTU/h donne 601 BTU/h.

Configuration d'une stratégie de limitation de puissance à l'aide de l'interface Web

Pour afficher et configurer des stratégies d'alimentation :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Alimentation/Thermique** → **Configuration de l'alimentation** → **Configuration de l'alimentation** . La page **Configuration de l'alimentation** s'affiche.

   La page **Configuration de l'alimentation** s'affiche. La limite de la stratégie d'alimentation actuelle figure dans la section **Stratégie de limite d'alimentation active**.
2. Sélectionnez **Activer** sous **Stratégie de limite d'alimentation iDRAC**.
3. Dans la section **Limites définies par l'utilisateur**, entrez la limite de puissance maximale en watts et en BTU/h ou le pourcentage maximal de limite système recommandée.
4. Cliquez sur **Appliquer** pour appliquer les valeurs.

Configuration d'une stratégie de limitation de l'alimentation à l'aide de l'interface RACADM

Pour afficher et définir les valeurs actuelles de limitation de l'alimentation :

- Utilisez les objets suivants avec la sous-commande **config** :
  - cfgServerPowerCapWatts

  - cfgServerPowerCapBTUhr
  - cfgServerPowerCapPercent
  - cfgServerPowerCapEnable
- Utilisation des objets suivants avec la sous-commande **set** :
  - System.Power.Cap.Enable
  - System.Power.Cap.Watts
  - System.Power.Cap.Btuhr
  - System.Power.Cap.Percent

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration d'une stratégie de limitation d'alimentation en utilisant l'utilitaire de configuration d'iDRAC

Pour afficher et configurer des stratégies d'alimentation :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Configuration de l'alimentation**.

   REMARQUE : Le lien **Configuration de l'alimentation** est disponible uniquement si l'unité d'alimentation du serveur prend en charge la surveillance de l'alimentation.

   La page **Paramètres iDRAC - Configuration de l'alimentation** s'affiche.
2. Sélectionnez **Activé** pour activer la **Stratégie de limite d'alimentation iDRAC.** Autrement, sélectionnez **Désactivé**.
3. Utilisez les paramètres recommandés, ou sous **Limites définies par l'utilisateur**, entrez les limites appropriées.
   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
4. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les valeurs de limitation de l'alimentation sont définies.

Configuration des options d'alimentation

Vous pouvez configurer les options d'alimentation, telles qu'une stratégie de redondance, le composant d'échange à chaud et la correction de facteur de puissance.

Le disque de secours est une fonction d'alimentation qui configure les unités d'alimentation pour qu'elles se mettent hors tension en fonction de la charge du serveur. Ceci permet aux unités d'alimentation restantes de fonctionner avec une charge plus élevée et plus efficacement. Pour cela, il est nécessaire que les unités d'alimentation prennent en charge cette fonction pour qu'elles se mettent sous tension rapidement lorsque cela est nécessaire.

Dans un système à deux UC, l'UC1 ou UC2 peut être configurée en tant qu'UC principale. Dans un système à quatre UC, vous devez définir la paire d'UC (1+1 ou 2+2) en tant qu'UC principale.

Une fois le disque de secours activé, les unités d'alimentation peuvent devenir actives ou se mettre en veille en fonction de la charge. Si le disque de secours est activé, le partage de courant électrique asymétrique entre les deux unités d'alimentation est activé. Une unité d'alimentation est *allumée* et fournit la majorité du courant ; l'autre unité est en mode veille et fournit une petite quantité de courant. Cette configuration de deux unités d'alimentation et d'un disque de secours activés est souvent appelée 1+0. Si toutes les unités d'alimentation 1 se trouvent sur le circuit A et que toutes les unités d'alimentation 2 se trouvent sur le circuit B, ce dernier a beaucoup moins de charge et déclenche les avertissements avec le disque de secours est activé (configuration d'usine du disque de secours par défaut). Si le disque de secours est désactivé, le courant électrique est partagé à 50/50 entre les deux unités d'alimentation, le circuit A et le circuit B ayant normalement la même charge.

Le facteur de puissance est le rapport de l'alimentation réelle consommée et de l'alimentation apparente. Lorsque la correction du facteur de puissance est activée, le serveur consomme une petite quantité d'alimentation lorsque l'hôte est désactivé. Par défaut, la correction du facteur d'alimentation est activée lorsque le serveur est expédié de l'usine.

Configuration des options d'alimentation en utilisant l'interface Web

Pour configurer les options d'alimentation :

1. Dans l'interface Web d'iDRAC7 accédez à **Présentation générale** → **Serveur** → **Alimentation/Thermique** → **Configuration de l'alimentation** → **Configuration de l'alimentation**. La page **Configuration de l'alimentation** s'affiche.
2. Sous **Options d'alimentation**, sélectionnez les options appropriées. Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer**. Les options d'alimentation sont configurées.

Configuration des options d'alimentation électrique à l'aide de l'interface RACADM

Pour configurer les options d'alimentation électrique, utilisez les objets suivants avec la sous-commande **set** :

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration des options d'alimentation à l'aide de l'utilitaire de configuration d'iDRAC

Pour configurer les options d'alimentation :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Configuration de l'alimentation**.

   REMARQUE : Le lien **Configuration de l'alimentation** est disponible uniquement si l'unité d'alimentation du serveur prend en charge la surveillance de l'alimentation.

   La page **Paramètres iDRAC - Configuration de l'alimentation** s'affiche.
2. Dans les options d'alimentation :
   - Activez ou désactivez la redondance d'alimentation.
   - Activez ou désactivez le composant de secours.
   - Définissez l'unité d'alimentation principale.
   - Activez ou désactivez la correction de facteur de puissance. Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

   Les options d'alimentation sont définies.

Activation ou désactivation du bouton Marche/Arrêt

Pour activer ou désactiver le bouton Marche/Arrêt du système géré :

1. Dans l'utilitaire Paramètres iDRAC, allez sous **Sécurité du panneau avant**.
   La page **Sécurité du panneau avant des paramètres iDRAC** s'affiche.
2. Sélectionnez **Activé** pour activer le bouton Marche/Arrêt ou bien sélectionnez **Désactivé**.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**. Les paramètres sont enregistrés.

12
Configuration et utilisation de la console virtuelle

Vous pouvez utiliser la console virtuelle pour gérer un système distant en utilisant le clavier, la vidéo et la souris sur la station de gestion pour contrôler les périphériques correspondants sur un serveur géré. Il s'agit d'une fonction disponible sous licence pour les serveurs en rack et de type tour. Elle est disponible par défaut dans les serveurs lames.

Les principales fonctions sont les suivantes :

- Jusqu'à quatre sessions de console virtuelle sont prises en charge. Toutes les sessions voient la même console de serveur géré simultanément.
- Vous pouvez lancer la console virtuelle dans un navigateur Web compatible en utilisant le plug-in Java ou ActiveX. Vous devez utiliser le visualiseur Java si la station de gestion fonctionne sur un système d'exploitation autre Windows.
- Lorsque vous ouvrez une session de console virtuelle, le serveur géré n'indique pas que la console a été redirigée.
- Vous pouvez ouvrir plusieurs sessions de console virtuelle depuis une même station de gestion sur un ou plusieurs systèmes gérés simultanément.
- Vous ne pouvez pas ouvrir deux sessions de console virtuelle depuis la station de gestion vers le serveur géré en utilisant le même plug-in.
- Si un second utilisateur demande une session de console virtuelle, la premier utilisateur est notifié et il peut refuser l'accès ou autoriser l'accès en lecture seule ou l'accès partagé complet. Le second utilisateur est averti que l'autre utilisateur détient le contrôle. Le premier utilisateur doit répondre dans un délai de trente secondes. Autrement, le second utilisateur obtient l'accès en fonction du paramétrage par défaut. Lorsque deux sessions sont actives simultanément, le premier utilisateur reçoit un message dans l'angle supérieur droit de l'écran indiquant que le second utilisateur a une session active. Si ni le premier utilisateur ni le second utilisateur ne disposent des privilèges d'administrateur, la fin de la session du premier utilisateur met fin automatiquement à celle du second.

Liens connexes

Configuration des navigateurs Web pour utiliser la console virtuelle
Configuration de la console virtuelle
Lancement de la console virtuelle

Résolutions d'écran et taux de rafraîchissement pris en charge

Le tableau suivant répertorie les résolutions d'écran prises en charge et les taux de rafraîchissement correspondants d'une session de console virtuelle exécutée sur le serveur géré.

Tableau 24. Résolutions d'écran prises en charge et taux de rafraîchissement correspondants

Résolution d'écran	Taux de rafraîchissement (Hz)
720 x 400	70
640 x 480	60, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1 024 x 768	60, 70, 72, 75, 85
1 280 x 1 024	60

Il est recommandé de configurer la résolution d'affichage minimale 1 280 x 1 024 sur le moniteur.

REMARQUE : Si vous une session de console virtuelle est active et qu'un écran d'une résolution inférieure est connecté à la console virtuelle, la résolution de la console du serveur peut être réinitialisée si le serveur est sélectionné sur la console locale. Si le système fonctionne sous un système d'exploitation Linux, une console X11 peut ne pas être visible sur l'écran local. Appuyez sur <Ctrl><Alt><F1> sur la console virtuelle iDRAC7 pour basculer Linux vers une console texte.

Configuration des navigateurs Web pour utiliser la console virtuelle

Pour utiliser la console virtuelle sur la station de gestion :

1. Assurez-vous qu'une version prise en charge du navigateur (Internet Explorer (Windows), ou Mozilla Firefox (Windows ou Linux), Google Chrome, Safari) est installée.

   Pour en savoir plus sur les versions de navigateur prises en charge, consultez le fichier *Lisez-moi* disponible à l'adresse **dell.com/support/manuals**.
2. Pour utiliser Internet Explorer, configurez Internet Explorer pour **Exécuter en tant qu'administrateur**.
3. Configurez le navigateur Web pour qu'il utilise le plug-in ActiveX ou Java.

   Le visualiseur ActiveX est compatible uniquement avec Internet Explorer. Un visualiseur Java est compatible avec tous les navigateurs.
4. Importez les certificats racine sur le système géré pour éviter les fenêtres contextuelles qui demandent de vérifier les certificats.
5. Installez le module associé **compat-libstdc++-33-3.2.3-61**.

   REMARQUE : Sur Windows, le module associé « compat-libstdc++-33-3.2.3-61 » peut être inclus dans le module .NET ou le module du système d'exploitation.
6. Si vous utilisez un système d'exploitation MAC, sélectionnez l'option **Activer l'accès aux périphériques d'aide** dans la fenêtre **Accès universel**.

   Pour en savoir plus, voir la documentation du système d'exploitation MAC.

Liens connexes

Configuration du navigateur Web pour utiliser le plug-in Java
Configuration d'IE pour qu'il utilise le plug-in ActiveX
Importation de certificats CA vers la station de gestion

Configuration du navigateur Web pour utiliser le plug-in Java

Installez un environnement JRE (Java Runtime Environment) si vous utilisez Firefox ou IE et voulez utiliser le visualiseur Java.

REMARQUE : Installez une version JRE 32 bits ou 64 bits sur un système d'exploitation 64 bits ou une version 32 bits sur un système d'exploitation 32 bits.

Pour configurer IE pour utiliser le plug-in Java :

- Désactivez les invites automatiques des téléchargements de fichiers dans Internet Explorer.
- Désactivez le *mode de sécurité renforcée* dans Internet Explorer.

Liens connexes

Configuration de la console virtuelle

Configuration d'IE pour qu'il utilise le plug-in ActiveX

Vous pouvez utiliser le plug-in ActiveX uniquement avec Internet Explorer.

Pour configurer IE pour qu'il utilise le plug-in ActiveX :

1. Effacez le cache du navigateur.
2. Ajoutez l'adresse IP ou le nom d'hôte d'iDRAC7 à la liste des **Sites de confiance**.
3. Réinitialisez les paramètres personnalisés pour les ramener à **Moyen bas** ou chargez les paramètres pour autoriser l'installation des plug-ins ActiveX signés.
4. Autorisez le navigateur à télécharger le contenu crypté et activer les extensions tierces du navigateur. Pour ce faire, accédez à **Outils** → **Options Internet** → **Avancé**, désélectionnez l'option **Ne pas enregistrer les pages cryptées sur le disque** et sélectionnez l'option **Activer les extensions tierce partie du navigateur**.

   REMARQUE : Redémarrez Internet Explorer pour appliquer le paramètre Activer les extensions tierce partie du navigateur.
5. Accédez à **Outils** → **Options Internet** → **Sécurité** et sélectionnez le fuseau horaire où vous voulez exécuter l'application.
6. Cliquez sur **Niveau personnalisé**. Dans la fenêtre **Paramètres de sécurité**, procédez comme suit :
   - Sélectionnez **Activé** pour **Demander confirmation pour les contrôles ActiveX**.
   - Sélectionnez **Demander** pour **Télécharger les contrôles ActiveX signés**.
   - Sélectionnez **Activé** ou **Demander** pour **Exécuter les contrôles ActiveX et les plug-ins**.
   - Sélectionnez **Activé** ou **Demander** pour **Contrôles ActiveX reconnus sûrs pour l'écriture de scripts**
7. Cliquez sur **OK** pour fermer la fenêtre **Paramètres de sécurité**.
8. Cliquez sur **OK** pour fermer la fenêtre **Options Internet**.

   REMARQUE : Avant d'installer le contrôle ActiveX, Internet Explorer peut afficher un avertissement de sécurité. Pour terminer l'installation d'ActiveX, acceptez le contrôle ActiveX lorsque Internet Explorer affiche un avertissement de sécurité.

Liens connexes

Effacement du cache du navigateur

Paramètres supplémentaires pour les systèmes d'exploitation Windows Vista ou Microsoft les plus récents

Paramètres supplémentaires pour les systèmes d'exploitation Windows Vista ou Microsoft les plus récents

Les navigateurs Internet Explorer intégrés à Windows Vista ou aux systèmes d'exploitation les plus récents sont dotés d'une fonction de sécurité supplémentaire appelée *Mode protégé*.

Pour lancer et exécuter des applications ActiveX dans les navigateurs Internet Explorer avec le *mode protégé* :

1. Exécutez IE en tant qu'administrateur.
2. Accédez à **Outils** → **Options Internet** → **Sécurité** → **Sites de confiance**.
3. Veillez à ne pas sélectionner l'option **Activer le mode protégé** dans la zone Site de confiance. Vous pouvez également ajouter l'adresse iDRAC7 aux sites dans la zone Intranet. Par défaut, le mode protégé est désactivé dans la zone Intranet et la zone Sites de confiance.
4. Cliquez sur **Sites**.
5. Dans le champ **Ajouter ce site Web à la zone**, ajoutez l'adresse de votre iDRAC7 et cliquez sur **Ajouter**.
6. Cliquez sur **Fermer**, puis sur **OK**.
7. Fermez et redémarrez le navigateur pour appliquer les paramètres.

Effacement du cache du 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 retirer ou supprimer les anciennes versions du Visualiseur susceptibles d'être stockées sur le système, puis réessayez.

REMARQUE : Vous devez disposer du privilège Administrateur pour pouvoir effacer la mémoire cache du navigateur.

Suppression des versions ActiveX antérieures dans IE7

Pour supprimer les anciennes versions du visualiseur Active-X pour IE7, procédez comme suit :

1. Fermez Video Viewer et le navigateur Internet Explorer.
2. Rouvrez Internet Explorer et accédez à **Internet Explorer → Outils → Gérer les modules complémentaires** et cliquez sur **Activer ou désactiver les modules complémentaires**. La fenêtre **Gérer les modules complémentaires** s'affiche.
3. Sélectionnez **Modules complémentaires qui ont été utilisés par Internet Explorer** dans le menu déroulant **Afficher**.
4. Supprimez le module complémentaire *Video Viewer*.

Suppression des versions ActiveX antérieures dans IE8

Pour supprimer les anciennes versions du Visualiseur Active-X pour IE8, procédez comme suit :

1. Fermez Video Viewer et le navigateur Internet Explorer.
2. Rouvrez 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.

Suppression des versions Java précédentes

Pour supprimer les anciennes versions du visualiseur Java sous Windows ou Linux, procédez comme suit :

1. Dans l'invite de commande, exécutez `javaws-viewer` ou `javaws-uninstall`
   Le **visualiseur Java Cache** s'affiche.
2. Supprimez les éléments intitulés *Client de console virtuelle iDRAC7*.

Importation de certificats CA vers la station de gestion

Lorsque vous lancez la console virtuelle ou Média Virtuel, des invites s'affichent pour vérifier les certificats. Si vous utilisez des certificats de serveur Web personnalisés, vous pouvez éviter ces invites en important les certificats vers la banque de certificats de confiance Java ou ActiveX.

Liens connexes

Importation d'un certificat CA vers la banque de certificats de confiance Java
Importation d'un certificat CA dans la banque de certificats de confiance ActiveX

Importation d'un certificat CA vers la banque de certificats de confiance Java

Pour importer le certificat CA dans la banque de certificats de confiance Java :

1. Démarrez le **Panneau de configuration Java**.
2. Cliquez sur l'onglet **Sécurité** et sur **Certificats**.
   La boîte de dialogue **Certificats** s'affiche.
3. Dans le menu déroulant de type de certificat, sélectionnez **Certificats de confiance**.

4. Cliquez sur **Importer**, accédez au certificat CA (dans le format codé en base 64), sélectionnez-le et cliquez sur **Ouvrir**.

   Le certificat sélectionné est importé dans la banque de certificats de confiance de démarrage Web.

5. Cliquez sur **Fermer** et sur **OK**. La fenêtre du **Panneau de configuration Java** se ferme.

Importation d'un certificat CA dans la banque de certificats de confiance ActiveX

Vous devez utiliser l'outil de ligne de commande SSL OpenSSL pour créer le hachage de certificat en utilisant SHA (Secure Hash Algorithm). Il est recommandé d'utiliser l'outil OpenSSL 1.0.x ou une version suivante, car il utilise SHA par défaut. Le certificat CA doit être au format PEM codé en base 64. Il s'agit d'un processus à exécution unique pour importer chaque certificat CA.

Pour importer le certificat CA dans la banque de certificats de confiance ActiveX :

1. Ouvrez l'invite de commande OpenSSL.
2. Exécutez un hachage de 8 octets sur le certificat CA en cours d'utilisation sur la station de gestion à l'aide de la commande `openssl x509 -in (nome de cert CA) -noout -hash`

   Un fichier de sortie est généré. Par exemple, si le fichier de certificat CA s'appelle **cacert.pem**, la commande est la suivante :

   ```
   openssl x509 -in cacert.pem -noout -hash
   ```

   Une sortie similaire à « 431db322 » est générée.
3. Renommez le fichier de certificat en utilisant le nom du fichier de sortie et incluez l'extension « 0 ». Par exemple, 431db322.0.
4. Copiez le certificat CA renommé dans votre répertoire de base. Par exemple, **C:\Documents and Settings \<utilisateur>**.

Configuration de la console virtuelle

Avant de configurer la console virtuelle, vérifiez que la station de gestion est configurée.

Vous pouvez configurer la console virtuelle à l'aide de l'interface Web iDRAC7 ou de l'interface de ligne de commande RACADM.

Liens connexes

Configuration des navigateurs Web pour utiliser la console virtuelle
Lancement de la console virtuelle

Configuration de la console virtuelle en utilisant l'interface Web

Pour configurer la console virtuelle en utilisant l'interface Web d'iDRAC7 :

1. Accédez à **Présentation générale → Serveur → Console virtuelle**. La page **Console Virtuelle** s'affiche.
2. Activez la console virtuelle et définissez les valeurs nécessaires. Pour plus d'information sur les options, voir l'*aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer**. La console virtuelle est configurée.

Configuration de la console virtuelle à l'aide de l'interface RACADM

Pour configurer la console virtuelle, utilisez l'une des méthodes suivantes :

- Utilisez les objets du groupe **iDRAC.VirtualConsole** avec la commande **set**.
- Utilisez les objets suivants avec la commande **config** :

- cfgRACTuneConRedirEnable
- cfgRACTuneConRedirPort
- cfgRACTuneConRedirEncryptEnable
- cfgRacTunePluginType
- cfgRacTuneVirtualConsoleAuthorizeMultipleSessions

Pour plus d'informations sur ces objets, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Prévisualisation de la console virtuelle

Avant de lancer la console virtuelle, vous pouvez prévisualiser son état sur la page **Système → Propriétés → Résumé du système**. La section de **Prévisualisation de la console virtuelle** contient une image indiquant l'état de la console virtuelle. L'image est actualisée toutes les 30 secondes. Il s'agit d'une fonction disponible sous licence.

REMARQUE : L'image de la console virtuelle est disponible uniquement si vous avez activé la console virtuelle.

Lancement de la console virtuelle

Vous pouvez lancer la console virtuelle à l'aide de l'interface Web d'iDRAC7 ou d'une URL.

REMARQUE : Ne lancez pas une session de console virtuelle depuis un navigateur Web sur le système géré.

Avant de lancer la console virtuelle, vérifiez que :

- Vous disposez des privilèges d'administrateur.
- Un navigateur Web est configuré pour utiliser le plug-in Java ou ActiveX.
- Une bande passante de 1 Mo/s est disponible.

REMARQUE : Si le contrôleur vidéo intégré est désactivé dans le BIOS et si vous lancez la console virtuelle, le Virtual Console Viewer (visualiseur de la console virtuelle) sera vide.

Lorsque vous lancez la console virtuelle en utilisant un navigateur 32 bits ou 64 bits, le plug-in (Java ou ActiveX) est disponible dans le navigateur. Les paramètres Options Internet sont communs aux deux navigateurs

Lorsque vous lancez la console virtuelle en utilisant le plug-in Java, une erreur de compilation Java peut se produire. Pour l'éliminer, accédez à **Panneau de configuration Java → Général → Paramètres réseau** et sélectionnez **Connexion directe**.

Si la console virtuelle est configurée pour utiliser le plug-in ActiveX, elle peut ne pas démarrer la première fois. Ceci s'explique par le fait que la connexion réseau est lente et que le délai d'expiration des données d'identification (utilisées par la console virtuelle pour la connexion) est de deux minutes. Le délai de téléchargement du plug-in du client ActiveX peut dépasser ce délai. Une fois le plug-in téléchargé, vous pouvez lancer la console normalement.

Lorsque vous lancez la console virtuelle pour la première fois en utilisant IE8 avec le plug-in ActiveX, le message « `Certificate Error: Navigation Blocked` » peut s'afficher. Cliquez sur **Poursuivre sur ce site Web** et sur **Installer** pour installer les contrôles ActiveX dans la fenêtre **Avertissement de sécurité**. La session de console virtuelle est lancée.

Liens connexes

Lancement de la console virtuelle en utilisant l'URL
Configuration du navigateur Web pour utiliser le plug-in Java
Configuration d'IE pour qu'il utilise le plug-in ActiveX
Lancement de la console virtuelle à l'aide de l'interface Web

Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX

Synchronisation des pointeurs des souris

Lancement de la console virtuelle à l'aide de l'interface Web

Vous pouvez lancer la console virtuelle des manières suivantes :

- Allez à **Présentation générale** → **Serveur** → **Console virtuelle**. La page **Console virtuelle** s'affiche. Cliquez sur **Lancer la console virtuelle**. Le **Visualiseur de console virtuelle** s'affiche.
- Allez à **Présentation générale** → **Serveur** → **Propriétés**. La page **Résumé du système** s'affiche. Dans la section **Prévisualisation de la console virtuelle**, cliquez sur **Lancer**. Le **Visualiseur de console virtuelle** démarre.

Le **Visualiseur de console virtuelle** affiche le bureau du système distant. Ce visualiseur permet de contrôler les fonctions de la souris et du clavier du système distant depuis la station de gestion.

Plusieurs boîtes de message peuvent s'afficher après le lancement de l'application. Pour interdire tout accès non autorisé à l'application, naviguez dans ces boîtes de message dans un délai de trois minutes pour éviter d'avoir à redémarrer l'application.

Si des fenêtres d'alerte de sécurité s'affichent lors du lancement du Visualiseur, cliquez sur Oui pour continuer.

Deux pointeurs de souris peuvent apparaître dans la fenêtre du visualiseur : un pour le serveur géré et un autre pour votre station de gestion. Pour synchroniser les curseurs, voir Synchronisation des pointeurs de souris.

Le lancement de la console virtuelle depuis une station de gestion Windows Vista peut générer des messages de redémarrage de console virtuelle. Pour éviter ces messages, définissez les valeurs d'expiration appropriées dans les emplacements suivants :

- **Panneau de configuration → Options d'alimentation → Économie d'énergie → Paramètres avancés → Disque dur → Mettre hors tension le disque dur après <délai>**
- **Panneau de configuration → Options d'alimentation → Hautes performances → Paramètres avancés → Disque dur → Mettre hors tension le disque dur après <délai d'expiration>**

Lancement de la console virtuelle en utilisant l'URL

Pour lancer la console virtuelle en utilisant l'URL :

1. Ouvrez un navigateur Web compatible et dans la zone d'adresse, tapez l'URL suivante en minuscules : **https://iDRAC7_adresse IP/console**
2. La page **Ouverture de session** correspondante s'affiche en fonction de la configuration d'ouverture de session :
   - Si la connexion directe est désactivée et que la connexion locale, Active Directory, LDAP ou par carte à puce est activée, la page **Ouverture de session** correspondante s'affiche.
   - Si la connexion directe est activée, le **Visualiseur de console virtuelle** s'ouvre et la page **Console virtuelle** s'affiche en arrière-plan.

   REMARQUE : Internet Explorer prend en charge les ouvertures de session locales, Active Directory, LDAP, par carte à puce (SC) et par connexion directe. Firefox prend en charge les ouvertures de session locales, AD et par connexion directe sur le système d'exploitation Windows, et locales, Active Directory et LDAP sur les systèmes d'exploitation Linux.

   REMARQUE : Si vous ne disposez pas des privilèges d'accès à la console virtuelle, cette URL lance Média Virtuel et non pas la console virtuelle.

Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX

Vous pouvez désactiver les messages d'avertissement lors du lancement de la console virtuelle ou du média virtuel en utilisant le plug-in Java.

1. Initialement, lorsque vous lancez la console virtuelle ou le média virtuel en utilisant le plug-in Java, l'invite pour vérifier l'éditeur s'affiche. Cliquez sur **Oui**.

   Un message d'avertissement de certificat s'affiche pour indiquer qu'un certificat de confiance est introuvable.

   REMARQUE : Si le certificat est trouvé dans le magasin de certificats du système d'exploitation ou s'il est détecté dans un emplacement d'utilisateur indiqué précédemment, ce message d'avertissement n'est pas affiché.

2. Cliquez sur **Continuer**.

   Le visualiseur de console virtuelle ou de média virtuel s'ouvre.

   REMARQUE : Le visualiseur du média virtuel est lancé si la console virtuelle est désactivée.

3. Dans le menu **Outils** , cliquez sur **Options de session** , puis sur l'onglet **Certificat** .
4. Cliquez sur **Rechercher le chemin**, spécifiez l'emplacement de stockage du certificat de l'utilisateur, cliquez sur **Appliquer**, puis sur **OK** et fermez le visualiseur.
5. Lancez la console virtuelle à nouveau.
6. Dans le message d'avertissement de certificat, sélectionnez l'option **Toujours faire confiance à ce certificat**, puis cliquez sur **Continuer**.
7. Quittez le visualiseur.
8. Lorsque vous relancez la console virtuelle, le message d'avertissement ne s'affiche pas.

Utilisation du Visualiseur de console virtuelle

Le visualiseur de la console virtuelle fournit différentes commandes telles que la synchronisation des souris, le facteur d'échelle de la console virtuelle, les options de clavardage, les macros de clavier, les actions d'alimentation, les périphériques de démarrage suivants et l'accès au média virtuel. Pour en savoir plus sur l'utilisation de ces fonctions, voir l'*aide en ligne iDRAC7*.

REMARQUE : Si le serveur distant est hors tension, le message « Aucun signal » s'affiche.

La barre de titre du Visualiseur de console virtuelle contient le nom DNS ou l'adresse IP de l'iDRAC7 auquel vous êtes connecté depuis la station de gestion. Si iDRAC7 n'a pas de nom DNS, l'adresse IP est affichée. Le format est :

- Pour les serveurs en rack et de type tour :
  `<nom DNS / adresse IPv6 / adresse IPv4>, <Modèle>, Utilisateur : <nom d'utilisateur>, <fps>`
- Pour les serveurs lames :
  `<nom DNS / adresse IPv6 / adresse IPv4>, <Modèle>, <Numéro de logement>, Utilisateur : <nom d'utilisateur>, <fps>`

Il peut arriver que le Visualiseur de console virtuelle affiche une vidéo de mauvaise qualité. Ceci est dû à la lenteur de la connectivité réseau qui provoque une perte d'une ou de deux trames vidéo lorsque vous démarrez la session de console virtuelle. Pour transmettre toutes les trames vidéo et améliorer la qualité vidéo, procédez de l'une des manières suivantes :

- Dans la page **Résumé du système**, dans la section **Prévisualisation de la console virtuelle**, cliquez sur **Actualiser**.

- Dans **Visualiseur de console virtuelle**, dans l'onglet **Performances**, amenez le curseur sur **Qualité vidéo maximale**.

Synchronisation des pointeurs des souris

Lorsque vous vous connectez à un système géré via la console virtuelle, la vitesse d'accélération de la souris sur le système géré peut ne pas se synchroniser avec le pointeur de la souris sur la station de gestion et deux pointeurs de souris s'affichent dans le Visualiseur.

Lorsque vous utilisez Red Hat Enterprise Linux ou Novell SUSE Linux, configurez le mode de la souris pour Linux avant de lancer le Visualiseur de console virtuelle. Les paramètres par défaut de la souris du système d'exploitation servent à contrôler la flèche de la souris dans le Visualiseur de console virtuelle.

Lorsque deux curseurs de souris apparaissent dans le visualiseur de la console virtuelle, cela signifie que le système d'exploitation du serveur prend en charge le positionnement relatif. Ceci est typique pour les systèmes d'exploitation Linux ou pour Lifecycle Controller - deux curseurs apparaissent si les paramètres d'accélération des souris du serveur sont différents des paramètres d'accélération des souris du client de la console virtuelle. Pour résoudre ce problème, passez à un curseur unique ou faites correspondre les paramètres d'accélération des souris du système géré et de la station de gestion :

- Pour passer à un curseur unique, sélectionnez **Curseur unique** dans le menu **Outils**.
- Pour définir les paramètres d'accélération des souris , rendez-vous sous **Outils → Options de session → Souris** . Sous l'onglet **Accélération de souris**, sélectionnez **Windows** ou **Linux**, en fonction du système d'exploitation.

Pour quitter le mode Curseur unique, appuyez sur la touche <Echap> ou sur la clé d'arrêt configurée.

REMARQUE : Ceci ne s'applique pas aux systèmes gérés qui exécutent le système d'exploitation Windows, car ils prennent en charge le positionnement absolu.

Lorsque vous utilisez la console virtuelle pour vous connecter à un système géré disposant d'un système d'exploitation Linux récent, des problèmes de synchronisation de souris peuvent apparaître. Ils sont provoqués par la fonction d'accélération de pointeur prévisible du bureau GNOME. Pour corriger la synchronisation de la souris dans la console virtuelle d'iDRAC7, désactivez cette fonction. Pour ce faire, dans la section de la souris du fichier **/etc/X11/xorg.conf**, ajoutez :

`Option "AccelerationScheme" "lightweight"`.

Si les problèmes de synchronisation persistent, effectuez les modifications supplémentaires suivantes dans le fichier **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** :

Remplacez les valeurs de `motion_threshold` et de `motion_acceleration` par `-1`.

Si vous désactivez l'accélération de la souris dans le bureau GNOME, dans le Visualiseur de console virtuelle, accédez à **Outils → Options de session → Souris** . Dans l'onglet **Accélération de la souris**, sélectionnez **Aucune**.

Pour un accès exclusif à la console du système géré, vous devez désactiver la console locale et affecter à **Sessions max.** la valeur `1` dans la page **Console Virtuelle**.

Envoi de toutes les frappes via la console virtuelle

Vous pouvez activer l'option **Envoyer toutes les frappes au serveur** et envoyer toutes les frappes et combinaisons de touches depuis la station de gestion au système géré via le visualiseur de la console virtuelle. Si cette option est désactivée, les combinaisons de touches sont redirigées vers la station de gestion sur laquelle la session de la console virtuelle s'exécute. Pour envoyer toutes les touches au serveur, dans le visualiseur de la console virtuelle, allez sous l'onglet **Outils → Options de session → Général** et sélectionnez l'option **Envoyer toutes les frappes au serveur** pour envoyer les frappes de la station de gestion au système géré.

Le comportement de la fonction Envoyer toutes les frappes au serveur dépend :

- du type de plug-in (Java ou ActiveX) en fonction duquel la session de console virtuelle est lancée ;

Pour le client Java, la bibliothèque native doit être chargée pour que l'option Envoyer toutes les frappes au serveur et le mode Curseur unique fonctionnent. Si les bibliothèques natives ne sont pas chargées, les options **Envoyer toutes les frappes au serveur** et **Curseur unique** sont désélectionnées. Si vous tentez de sélectionner l'une de ces options, un message d'erreur s'affiche indiquant que les options sélectionnées ne sont pas prises en charge.

Pour le client ActiveX, la bibliothèque doit être chargée pour que la fonction Envoyer toutes les frappes au serveur fonctionne. Si les bibliothèques natives ne sont pas chargées, l'option **Envoyer toutes les frappes au serveur** est désélectionnée. Si vous tentez de sélectionner cette option, un message d'erreur s'affiche indiquant que la fonction n'est pas prise en charge.

Pour les systèmes d'exploitation MAC, activez l'option **Activer l'accès pour les périphériques d'aide** dans **Accès universel** pour que la fonction Envoyer toutes les frappes au serveur fonctionne.

- du système d'exploitation de la station de gestion et de celui du système géré. Les combinaisons de touches significatives pour le système d'exploitation de la station de gestion ne sont pas envoyées au système géré ;
- du mode du Visualiseur de console virtuelle ; Avec fenêtres ou Plein écran.

  En mode Plein écran, l'option **Envoyer toutes les frappes au serveur** est activée par défaut.

  En mode Avec fenêtres, les touches sont envoyées uniquement lorsque le Visualiseur de console virtuelle est visible et actif.

  Lorsque vous passez du mode Plein écran au mode Avec fenêtres, l'état précédent de l'envoi de toutes les touches est réactivé.

Liens connexes

Session de console virtuelle Java-sur le système d'exploitation Windows
Session de console virtuelle Java exécutée sur le système d'exploitation Linux
Session de console virtuelle ActiveX sur le système d'exploitation Windows

Session de console virtuelle Java-sur le système d'exploitation Windows

- La touche Ctrl+Alt+Suppr n'est pas envoyée au système géré, mais elle est toujours interprétée par la station de gestion.
- Lorsque l'envoi de toutes les frappes au serveur est activé, les touches suivantes ne sont pas envoyées au système géré :
  - Touche Précédent du navigateur
  - Touche Suivant du navigateur
  - Touche Actualiser du navigateur
  - Touche Arrêt du navigateur
  - Touche de recherche du navigateur
  - Touche Favoris du navigateur
  - Touche de démarrage et Origine du navigateur
  - Touche de coupure du son
  - Touche de diminution du volume
  - Touche d'augmentation du volume
  - Touche Piste suivante
  - Touche Piste précédente
  - Touche Arrêt média
  - Touche Lecture/Pause
  - Touche Démarrage de la messagerie
  - Touche Sélection de média
  - Touche Application 1

  - Touche Application 2
- Toutes les touches individuelles (non pas une combinaison de touches, mais une seule frappe de touche) sont toujours envoyées au système géré. Ceci inclut toutes les touches de fonction, les touches Maj, Alt, Ctrl et les touches Menu. Certaines de ces touches affectent la station de gestion et le système géré.

  Par exemple, si la station de gestion et le système géré utilisent le système d'exploitation Windows et que l'envoi de toutes les touches est désactivé, lorsque vous appuyez sur la touche Windows pour ouvrir le menu **Démarrer**, le menu **Démarrer** s'ouvre sur la station de gestion et le système géré. Cependant, si l'envoi de toutes les touches est activé, le menu **Démarrer** s'ouvre sur le système géré, mais pas sur la station de gestion.
- Lorsque l'envoi de toutes les touches est désactivé, le comportement dépend des combinaisons de touches utilisées et des combinaisons spéciales interprétées par le système d'exploitation sur la station de gestion.

Session de console virtuelle Java exécutée sur le système d'exploitation Linux

Le comportement mentionné pour le système d'exploitation Windows s'applique également au système d'exploitation Linux avec les exceptions suivantes :

- Lorsque l'envoi de toutes les frappes au serveur est activé, <Ctrl+Alt+Suppr> est envoyé au système d'exploitation du système géré.
- Les touches Magic SysRq sont des combinaisons de touches interprétées par Linux Kernel. Elles sont utiles si le système d'exploitation du système géré de la station de gestion ou du système géré se bloque et que vous devez récupérer le système. Vous pouvez activer les touches magiques SysRq sur le système d'exploitation Linux en utilisant les méthodes suivantes :
  - Ajoutez une entrée à **/etc/sysctl.conf**
  - echo 1 > /proc/sys/kernel/sysrq
- Lorsque l'envoi de toutes les touches au serveur est activé, les touches magiques SysRq sont envoyées au système d'exploitation du système géré. Le comportement de la séquence de touches pour réinitialiser le système, à savoir redémarrer sans démontage ou synchronisation, varie selon que SysRq est activé ou désactivé sur la station de gestion :
  - Si SysRq et activé sur la station de gestion, <Ctrl+Alt+SysRq+b> ou <Alt+SysRq+b> réinitialise la station de gestion, quel que soit l'état du système.
  - Si SysRq est désactivé, les touches <Ctrl+Alt+SysRq+b> ou <Alt+SysRq+b> réinitialisent le système d'exploitation du système géré.
  - Les autres combinaisons de touches SysRq (telles que, <Alt+SysRq+k>, <Ctrl+Alt+SysRq+m>, etc.) sont envoyées au système géré, que les touches SysRq soient activées ou non sur la station de gestion.

Session de console virtuelle ActiveX sur le système d'exploitation Windows

Le comportement de l'envoi de toutes les frappes au serveur dans une session de console virtuelle ActiveX exécutée sur le système d'exploitation Windows est similaire au comportement expliqué pour une session de console virtuelle Java sur la station de gestion, mais avec les exceptions suivantes :

- Lorsque l'envoi de toutes les touches est désactivé et que vous appuyez sur F1, vous affichez l'aide de l'application sur la station de gestion et le système géré et le message suivant s'affiche :

  ```
  Cliquez sur Aide sur la page Console Virtuelle pour afficher l'aide en ligne.
  ```
- Les touches de média peuvent ne pas être bloquées de manière explicite.
- Les combinaisons de touches <Alt + Espace>, <Ctrl + Alt + +>, <Ctrl + Alt + -> ne sont pas envoyées au système géré et elles sont interprétées par le système d'exploitation de la station de gestion.

13

Gestion de Média Virtuel

Média Virtuel permet au serveur géré d'accéder aux périphériques de support sur la station de gestion ou aux images de CD/DVD ISO sur un partage de réseau comme s'il s'agissait de périphériques sur le serveur géré.

Avec la fonction Média Virtuel, vous pouvez :

- Accéder à distance à un support connecté à un système distant sur le réseau
- Installer des applications
- Mettre à jour les pilotes
- Installer un système d'exploitation sur le système géré

Il s'agit d'une fonction sous licence pour les serveurs en rack ou de type tour. Elle est disponible par défaut sur les serveurs lames.

Les principales fonctions sont :

- Prise en charge des lecteurs optiques virtuels (CD/DVD), des lecteurs de disquette (y compris les lecteurs USB) et des lecteurs Flash USB.
- Vous pouvez connecter un seul lecteur de disquette, lecteur Flash USB, image ou clé et un seul lecteur optique dans la station de gestion à un système géré. Les lecteurs de disquette pris en charge incluent une image de disquette ou un lecteur de disquette disponible. Les lecteurs optiques pris en charge incluent un seul lecteur optique maximum disponible ou un seul fichier image ISO.

  L'illustration suivante montre une configuration Média Virtuel type.
- Le lecteur de disquette virtuel d'iDRAC7 n'est pas accessible depuis les machines virtuelles.
- Un média virtuel connecté émule un périphérique physique sur le système géré.
- Sur les système gérés Windows, les lecteurs Média Virtuel sont montés automatiquement s'ils sont connectés et configurés avec une lettre d'unité.
- Sur les systèmes gérés Linux avec certaines configurations, les lecteurs Média Virtuel ne sont pas montés automatiquement. Pour monter les lecteurs manuellement, utilisez la commande mount.
- Toutes les demandes d'accès aux lecteurs virtuels du système géré sont envoyées à la station de gestion dans le réseau.
- Les périphériques virtuels apparaissent comme deux lecteurs sur le système géré sans que le support soit installé dans les lecteurs.
- Vous pouvez partager le lecteur de CD/DVD (lecture seule) de la station de gestion, mais pas un média USB, entre deux systèmes gérés.
- Média Virtuel exige une bande passante réseau disponible d'au moins 128 Kb/s.
- Si un basculement LOM ou NIC se produit, la session Média Virtuel est déconnectée.

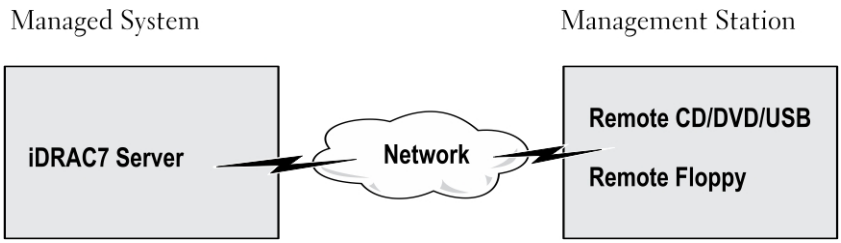

Figure 4. Configuration Média Virtuel

Lecteur et périphériques compatibles

Le tableau suivant répertorie les lecteurs compatibles via Média Virtuel.

Tableau 25. Lecteur et périphériques compatibles

Lecteur	Support de stockage compatible
Lecteurs optiques virtuels	• Lecteur de disquette 1,44 hérité avec disquette 1,44 • CD-ROM • DVD • CD-RW • Lecteur avec support CD-RO
Lecteurs de disquette virtuels	• Fichier image de CD-ROM/DVD au format ISO9660 • Fichier image de disquette ISO9660 au format ISO9660
Lecteurs Flash USB	• Lecteur de CD-ROM USB avec support CD-ROM • Fichier image USB au format ISO9660

Configuration de Média Virtuel

Avant de définir les paramètres Média Virtuel, configurez le navigateur Web pour utiliser le plug-in Java ou ActiveX

Liens connexes

Configuration des navigateurs Web pour utiliser la console virtuelle

Configuration de Média Virtuel en utilisant l'interface Web d'iDRAC7

Pour définir les paramètres Média Virtuel :

PRÉCAUTION : Ne réinitialisez pas iDRAC7 lorsque vous exécutez une session Média Virtuel afin de ne pas obtenir des résultats indésirables, notamment une perte de données.

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Média connecté**.
2. Définissez les paramètres nécessaires. Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration de Média Virtuel en utilisant l'interface RACADM

Pour configurer le média virtuel :

- Utilisez les objets du groupe **iDRAC.VirtualMedia** avec la commande **set**.
- Utilisez les objets du groupe **cfgRacVirtual** avec la commande **config**.

Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Configuration de Média Virtuel à l'aide de l'utilitaire de configuration d'iDRAC

Vous pouvez connecter, déconnecter ou connecter automatiquement un média virtuel en utilisant l'utilitaire de configuration d'iDRAC. Pour ce faire :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Média Virtuel**.
   La page **Paramètres iDRAC- Média Virtuel** s'affiche.
2. Sélectionnez **Déconnecter**, **Connecter** ou **Connecter automatiquement** en fonction des besoins. Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d''iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres du média virtuel sont configurés.

État Média connecté et réponse du système

Le tableau suivant indique la réponse du système en fonction du paramètre Média connecté.

Tableau 26. État de support connecté et réponse du système

État de média connecté	Réponse du système
Déconnecter	Impossible de mapper une image au système.
Connecter	Le média est mappé, même lorsque la **Vue Client** est fermée.
Connecter automatiquement	Le média est mappé lorsque la **Vue Client** est ouverte et démappé lorsque la **Vue Client** est fermée.

Accès à Média Virtuel

Vous pouvez accéder au média virtuel avec ou sans la console virtuelle. Avant d'accéder au média virtuel, veillez à configurer les navigateurs Web.

Le média virtuel et RFS sont mutuellement exclusifs. Si la connexion RFS est active et que vous tentez de lancer le client média virtuel, le message d'erreur suivant s'affiche : *Le média virtuel est actuellement indisponible. Une session média virtuel ou de partage de fichiers à distance est en cours d'utilisation.*

Si la connexion RFS n'est pas active, et que vous tentez de lancer le client média virtuel, celui-ci est lancé avec succès. Vous pouvez alors utiliser le client média virtuel pour mapper des périphériques et des fichiers aux lecteurs virtuels du média virtuel.

Liens connexes

Configuration des navigateurs Web pour utiliser la console virtuelle
Configuration de Média Virtuel

Lancement de Média Virtuel à l'aide de la console virtuelle

Avant de lancer Média Virtuel via la console virtuelle, vérifiez que :

- La console virtuelle est activée..
- Le système est configuré pour ne pas masquer les lecteurs vides - Dans l'Explorateur Windows, accédez à **Options des dossiers**, désélectionnez l'option **Masquer les disques vides dans le dossier de l'ordinateur**, puis cliquez sur **OK**.

Pour accéder à Média Virtuel en utilisant la console virtuelle :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale → Serveur → Console virtuelle**.
   La page **Console virtuelle** s'affiche.
2. Cliquez sur **Lancer Console virtuelle**.
   Le **Visualiseur de console virtuelle** s'ouvre.

   REMARQUE : Sous Linux, Java est le type de plug-in par défaut pour accéder à la console virtuelle. Sous Windows, ouvrez le fichier **.jnlp** pour lancer la console virtuelle à l'aide de Java.
3. Cliquez sur **Média Virtuel → Lancer Média Virtuel**.
   La session de média virtuel est établie et le menu **Média virtuel** affiche la liste des périphériques disponibles en vue du mappage.

   REMARQUE : La fenêtre du **Visualiseur de console virtuelle** doit rester active pendant que vous accédez à Média Virtuel.

   .

Liens connexes

Configuration des navigateurs Web pour utiliser la console virtuelle
Configuration de Média Virtuel
Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX

Lancement de Média Virtuel sans utiliser la console virtuelle

Avant de lancer Média Virtuel lorsque la **Console virtuelle** est désactivée, vérifiez que :

- Média Virtuel est *connecté*.
- Le système est configuré pour afficher les lecteurs vides. Pour ce faire, dans l'Explorateur Windows, accédez à **Options de dossier**, désélectionnez l'option **Masquer les lecteurs vides dans le dossier Ordinateur**, puis cliquez sur **OK**.

Pour lancer Média Virtuel lorsque la console virtuelle est désactivée :

1. Dans l'interface Web d'iDRAC7, allez à **\Présentation générale → Serveur → Console virtuelle**.
   La page **Console virtuelle** s'affiche.
2. Cliquez sur **Lancer Console virtuelle**.
   Le message suivant s'affiche :

   ```
   Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
   ```
3. Cliquez sur **OK**.
   La fenêtre **Média virtuel** s'affiche.
4. Dans le menu **Média virtuel** , cliquez sur **Mappage du CD/DVD** ou **Mappage de disque amovible**.
   Pour plus d'informations, reportez-vous à la section Mappage de lecteur virtuel.

   REMARQUE : Les lettres de lecteur de périphérique virtuel sur le système géré ne coïncident pas avec les lettres de lecteur physique sur la station de gestion.

   REMARQUE : Média Virtuel peut ne pas fonctionner correctement sur les clients du système d'exploitation Windows configurés avec la sécurité renforcée d'Internet Explorer. Pour résoudre le problème, voir la documentation du système d'exploitation ou contacter l'administrateur système.

Liens connexes

Configuration de Média Virtuel

Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX

Ajout d'images Média Virtuel

Vous pouvez créer une image média du dossier à distance et la monter en tant que périphérique USB connecté sur le système d'exploitation du serveur. Pour ajouter des images de média virtuel :

1. Cliquez sur **Média virtuel** → **Créer une image...**.
2. Dans le champ **Dossier source**, cliquez sur **Parcourir** et naviguez vers le dossier ou le répertoire à utiliser comme source du fichier image. Le fichier image se trouve sur la station de gestion ou sur le lecteur C: du système géré.
3. Dans le champ **Nom du fichier d'image**, le chemin d'accès par défaut au stockage des fichiers d'image créés (en règle générale, le répertoire du bureau) apparaît. Pour changer cet emplacement, cliquez sur **Parcourir** et recherchez un emplacement.
4. Cliquez sur **Créer une image**.

   Le processus de création d'image démarre. Si l'emplacement du fichier d'image se trouve au sein du dossier source, le message d'avertissement qui s'affiche indique que la création d'image ne peut pas se poursuivre car l'emplacement du fichier d'image au sein du dossier source crée une boucle à l'infini. Si l'emplacement du fichier d'image ne se trouve pas au sein du dossier source, la création de l'image se poursuit.

   Une fois l'image créée, un message indiquant que la création a réussi s'affiche.
5. Cliquez sur **Terminer**.

   L'image est créée.

   Lorsque le dossier est ajouté comme image, un fichier **.img** est créé sur le bureau de la station de gestion d'où la fonction est utilisée. Si ce fichier **.img** est déplacé ou supprimé, l'entrée correspondante du dossier dans le menu **Média Virtuel** ne fonctionne pas. Par conséquent, il est recommandé de ne pas déplacer ni de supprimer le fichier **.img** lorsque l'*image* est en cours d'utilisation. Toutefois, le fichier **.img** peut être supprimé après désélection de l'entrée appropriée et en utilisant la commande de **suppression d'image** pour supprimer l'entrée.

Affichage des informations d'un périphérique virtuel

Pour afficher les détails du périphérique virtuel, dans le visualiseur de console virtuelle, cliquez sur **Outils** → **Statistiques**. Dans la fenêtre **Statistiques** , la section **Média virtuel** affiche les périphériques virtuels mappés et l'activité de lecture/écriture correspondant à chaque périphérique. Si le média virtuel est connecté, ces informations s'affichent. Si le média virtuel n'est pas connecté, le message « Média virtuel non connecté » s'affiche.

Si le média virtuel est lancé sans l'aide de la console virtuelle, la section **Média virtuel** apparaît sous forme de boîte de dialogue. Elle fournit des informations sur les périphériques mappés.

Réinitialisation USB

Pour réinitialiser le périphérique USB :

1. Dans le visualiseur de console virtuelle, cliquez sur **Outils** → **Statistiques**.

   La fenêtre de **Statistiques** s'affiche.
2. Dans la section **Média virtuel**, cliquez sur **Réinitialisation USB**.

   Un message affiche un avertissement à l'attention de l'utilisateur pour lui indiquer que la réinitialisation de la connexion USB peut affecter toutes les entrées vers le périphérique cible, y compris Média Virtuel, le clavier et la souris.

3. Cliquez sur **Oui**.

   L'USB est réinitialisé.

   REMARQUE : Média Virtuel iDRAC7 ne prend pas fin, même après que vous vous déconnectez de la session d'interface Web iDRAC7.

Mappage d'un lecteur virtuel

Pour mapper un lecteur virtuel :

REMARQUE : Lorsque vous utilisez Média Virtuel ActiveX, vous devez disposer des privilèges administratifs pour pouvoir mapper un DVD ou un lecteur Flash USB de système d'exploitation (connecté à la station de gestion). Pour mapper le lecteur, lancez IE en tant qu'administrateur ou ajoutez l'adresse IP d'iDRAC7 à la listes des sites de confiance.

1. Pour établir une session de média virtuel, à partir du menu **Média virtuel**, cliquez sur **Connecter le média virtuel**.

   Pour chaque périphérique disponible pour mappage depuis le serveur hôte, un élément de menu apparaît sous le menu **Média virtuel**. Cet élément porte le nom du type de périphérique, par exemple :

   - Mapper CD/DVD
   - Mapper le disque amovible
   - Mapper une disquette

   REMARQUE : L'élément de menu **Mappage du lecteur de disquette** apparaît dans la liste si l'option **Émulation de disquette** est activée sur la page de **média connecté**. Quand **Émulation de disquette** est activée, **Mappage du disque amovible** est remplacé par **Mappage du lecteur de disquette**.

2. Cliquez sur le type de périphérique que vous souhaitez mapper.

   REMARQUE : La session active indique si une session de média virtuel est actuellement active à partir de la session d'interface Web actuelle, à partir d'une autre session d'interface Web ou à partir de VMCLI.

3. Dans le champ **Lecteur/Fichier d'image**, sélectionnez le périphérique dans la liste déroulante.

   La liste contient tous les périphériques disponibles (non mappés) que vous pouvez mapper (CD/DVD, Disque amovible, Lecteur de disquette) et les types de fichier d'image que vous pouvez mapper (ISO ou IMG). Les fichiers d'image se trouvent dans le répertoire de fichiers d'image par défaut (en règle générale, le bureau de l'utilisateur). Si le périphérique n'est pas disponible dans la liste déroulante, cliquez sur **Parcourir** pour le spécifier.

   Le bon type de fichier pour CD/DVD est ISO, et IMG pour disquette et disque amovible.

   Lorsque l'image est créée dans le chemin par défaut (ordinateur de bureau), lorsque vous sélectionnez **Mappage de disque amovible**, l'image créée est disponible pour être sélectionnée dans le menu déroulant.

   Si l'image est créée dans un autre emplacement, lorsque vous sélectionnez **Mappage de disques amovibles**, l'image créée n'est pas disponible dans le menu déroulant. Cliquez sur **Parcourir** pour spécifier l'image.

4. Sélectionnez **lecture seule** pour mapper les périphériques enregistrables en lecture seule.

   Pour les périphériques CD/DVD, cette option est activée par défaut et vous ne pouvez pas la désactiver.

5. Cliquez sur **Mapper le périphérique** pour mapper le périphérique au serveur hôte.

   Une fois le périphérique/fichier mappé, le nom de son élément de menu **Média virtuel** change pour refléter le nom du périphérique. Par exemple, si le périphérique CD/DVD est mappé sur un fichier image nommé **foo.iso**, l'élément du menu CD/DVD du menu Média virtuel se nomme **foo.iso mappé sur le CD/DVD**. Une coche en regard de cet élément de menu indique qu'il est mappé.

Liens connexes

Affichage des lecteurs virtuels corrects pour le mappage

Ajout d'images Média Virtuel

Affichage des lecteurs virtuels corrects pour le mappage

Sur une station de gestion Linux, la fenêtre du **Client** de Média Virtuel peut contenir des lecteurs de disque et de disquette qui ne font pas partie de la station de gestion. Pour que les lecteurs virtuels corrects soient disponibles pour le mappage, vous devez activer le paramétrage de port du disque dur ATA connecté. Pour ce faire :

1. Redémarrez le système d'exploitation sur la station de gestion. Au cours du POST, appuyez sur <F2> ou <F12> pour entrer dans le programme de configuration du système.
2. Accédez à **Paramètres SATA**. Les informations de port s'affichent.
3. Activez les ports présents et connectés au disque dur.
4. Accédez à la fenêtre du **Client** de Média Virtuel. Elle contient les lecteurs corrects qui peuvent être mappés.

Liens connexes

Mappage d'un lecteur virtuel

Dissociation d'un lecteur virtuel

Pour dissocier un lecteur virtuel :

1. Dans le menu **Média virtuel**, effectuez l'une des opérations suivantes :
   - Cliquez sur le périphérique dont vous voulez supprimer le mappage.
   - Cliquez sur **Déconnecter le média virtuel**.

   Un message s'affiche vous demandant de confirmer.
2. Cliquez sur **Oui**.
   La case à cocher correspondant à cet élément de menu ne s'affiche pas, ce qui signifie qu'il n'existe aucun mappage sur le serveur hôte.

Définition de la séquence de démarrage via le BIOS

En utilisant l'utilitaire System BIOS Settings, vous pouvez configurer le système géré pour qu'il démarre depuis les lecteurs optiques virtuels ou les lecteurs de disquette virtuels.

REMARQUE : Le changement de Média Virtuel en cours de connexion peut interrompre la séquence de démarrage du système.

Pour permettre au système géré de démarrer :

1. Démarrez le système géré.
2. Appuyez sur <F2> pour accéder à la page **Configuration du système**.
3. Accédez à **Paramètres du BIOS du système** → **Paramètres de démarrage** → **Paramètres de démarrage du BIOS** → **Séquence de démarrage**.
   Dans la fenêtre contextuelle, les lecteurs optiques virtuels et les lecteurs de disquette virtuels sont répertoriés avec les périphériques de démarrage standard.
4. Vérifiez que le lecteur virtuel est activé et qu'il est le premier périphérique avec un support amorçable. Si nécessaire, suivez les instructions qui s'affichent pour modifier la séquence de démarrage.
5. Cliquez sur **OK**, revenez à la page **System BIOS Settings** et cliquez sur **Terminer**.

6. Cliquez sur **Oui** pour enregistrer les modifications et quitter.

   Le système géré redémarre.

   Il tente de démarrer depuis un périphérique amorçable en fonction de la séquence de démarrage. Si le périphérique virtuel est connecté et qu'un support amorçable est présent, le système démarre depuis le périphérique virtuel. Dans le cas contraire, il ignore le périphérique comme dans le cas d'un périphérique physique ne contenant pas de support amorçable.

Activation du démarrage unique pour Média Virtuel

Vous pouvez changer la séquence de démarrage uniquement une fois lorsque vous démarrez le système après avoir connecté un périphérique Média Virtuel distant.

Avant d'activer l'option de démarrage unique :

- Vérifiez que vous disposez du privilège de *configuration d'utilisateur*.
- Associez les lecteurs locaux ou virtuels (CD/DVD, lecteur de disquette ou lecteur Flash USB) au média ou à l'image amorçable en utilisant les options Média Virtuel.
- Média Virtuel est *connecté* pour que les lecteurs virtuels apparaissent dans la séquence de démarrage.

Pour activer l'option de démarrage unique et démarrer le système géré depuis Média Virtuel :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Média connecté**.
2. Sous **Média Virtuel**, sélectionnez **Activer le démarrage unique** et cliquez sur **Appliquer**.
3. Allumez le système géré et appuyez sur **<F2>** pendant le démarrage.
4. Modifiez la séquence de démarrage afin de démarrer à partir du périphérique Média Virtuel distant.
5. Redémarrez le serveur.

   Le système géré démarre une fois depuis le média virtuel.

Liens connexes

Mappage d'un lecteur virtuel
Configuration de Média Virtuel

14

Installation de l'utilitaire VMCI

L'utilitaire WMCLI (Virtual Media Command Line Interface) est une interface qui fournit des fonctions de média virtuel de la station de gestion vers iDRAC7 sur le système géré. Utilisez cet utilitaire pour accéder aux fonctions de média virtuel, notamment aux fichiers images et aux lecteurs physiques, pour déployer un système d'exploitation sur plusieurs systèmes distants dans un réseau.

REMARQUE : Vous pouvez exécuter l'utilitaire VMCLI uniquement sur la station de gestion qui est installée avec le système d'exploitation 32 bits.

L'utilitaire VMCLI prend en charge les fonctionnalités suivantes :

- Gestion des périphériques amovibles ou des images accessibles via Média Virtuel.
- Fin de la session lorsque l'option **Démarrage unique** du micrologiciel iDRAC7 est activée.
- Sécurisation des communications vers iDRAC7 à l'aide du protocole SSL (Secure Sockets Layer)
- Exécutez les commandes VMCLI jusqu'à ce que :
  - Les connexions se terminent automatiquement.
  - Un système d'exploitation termine le processus.

  REMARQUE : Pour mettre fin au processus dans Windows, utilisez le Gestionnaire des tâches.

Installation de VMCLI

L'utilitaire VMCLI est inclus dans le DVD *Dell Systems Management Tools and Documentation*.

Pour installer l'utilitaire VMCLI :

1. Insérez le DVD *Dell Systems Management Tools and Documentation* dans le lecteur de DVD.
2. Suivez les instructions qui s'affichent pour installer les outils DRAC.
3. Après l'installation, vérifiez le dossier **install\Dell\SysMgt\rac5** pour vous assurer que **vmcli.exe** existe. De même, vérifiez le chemin pour UNIX.

   L'utilitaire VMCLI est installé sur le système.

Exécution de l'utilitaire VMCLI

- Si le système d'exploitation nécessite des privilèges spécifiques ou d'appartenir à un groupe, vous devez disposer de privilèges similaires pour pouvoir exécuter des commandes VMCLI.
- Sur les systèmes Windows, les utilisateurs non-administrateurs doivent avoir les privilèges **Utilisateur avec pouvoir** pour pouvoir exécuter l'utilitaire VMCLI.
- Sur les systèmes Linux, pour accéder à iDRAC7 et exécuter VMCLI et les commandes utilisateur d'ouverture de session, les utilisateurs non-administrateurs doivent utiliser `sudo` comme préfixe dans les commandes VMCLI. Toutefois, pour ajouter ou modifier des utilisateurs dans le groupe Administrateurs VMCLI, utilisez la commande `visudo`.

Syntaxe VMCLI

L'interface VMCLI est identique sur les systèmes Windows et Linux. La syntaxe VMCLI est la suivante :

```
VMCLI [paramètre] [options d'environnement du système d'exploitation]
```

Par exemple, `vmcli -r iDRAC7 adresse IP:iDRAC7 port SSL`

Le *paramètre* -r permet à VMCLI de se connecter au serveur défini, d'accéder à iDRAC7et de se mapper au support virtuel spécifié.

REMARQUE : La syntaxe VMCLI tient compte de la casse.

À des fins de sécurité, il est recommandé d'utiliser les paramètres VMCLI suivants :

- `vmcli -i` : permet d'utiliser une méthode interactive pour démarrer VMCLI. Elle permet de masquer le nom d'utilisateur et le mot de passe lorsque les processus sont examinés par d'autres utilisateurs.
- vmcli `-r <iDRAC7 adresse IP[:iDRAC7 port SSL]> -S -u <iDRAC7-nom d'utilisateur> -p <iDRAC7-mot de passe> -c {<nom du périphérique> | <fichier image>}` — Indique si le certificat CA iDRAC7 est valide. Si le certificat n'est pas valide, un message d'avertissement s'affiche lorsque vous exécutez la commande. Cependant, la commande aboutit et une session VMCLI est établie. Pour plus d'informations sur les paramètres VMCLI, voir l'*Aide VMCLI* ou les *Pages Man VMCLI*.

Liens connexes

Commandes VMCLI pour accéder à Média Virtuel
Options VMCLI d'environnement de système d'exploitation

Commandes VMCLI pour accéder à Média Virtuel

Le tableau suivant répertorie les commandes VMCLI nécessaires pour accéder à un média virtuel différent.

Tableau 27. Commandes VMCLI

Média Virtuel	Commande
Lecteur de disquette	`vmcli -r [adresse IP ou nom d'hôte RAC] -u [nom d'utilisateur iDRAC7] -p [mot de passe iDRAC7] -f [nom du périphérique]`
Disquette amorçable ou image de clé USB	`vmcli -r [adresse IP iDRAC7] [nom d'utilisateur iDRAC7] -p [mot de passe iDRAC7] -f [floppy.img]`
Lecteur de CD en utilisant l'option -f	`vmcli -r [adresse IP iDRAC7] -u [nom d'utilisateur iDRAC7] -p [mot de passe iDRAC7] -f [nom de périphérique]| [fichier image]-f [cdrom - dev ]`
Image CD/DVD amorçable	`vmcli -r [adresse IP iDRAC7] [nom d'utilisateur iDRAC7] -p [mot de passe iDRAC7] -f [floppy.img]`

Si le fichier n'est pas protégé contre l'écriture, Média Virtuel peut écrire dans le fichier image. Pour que Média Virtuel n'écrive pas sur le support :

- Configurez le système d'exploitation pour protéger contre l'écriture un fichier image de disquette qui ne doit pas être remplacé.

- Utilisez la fonction de protection contre l'écriture du périphérique.

Lors de la virtualisation des fichiers images en lecture seule, plusieurs sessions peuvent utiliser simultanément le même support d'image.

Lors de la virtualisation des lecteurs physiques, une seule session peut accéder à un lecteur physique donné à la fois.

Options VMCLI d'environnement de système d'exploitation

VMCLI utilise des options d'environnement pour activer les fonctions suivantes de système d'exploitation :

- 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, remplace le fichier indiqué par la sortie imprimée de l'utilitaire VMCLI.

  REMARQUE : L'utilitaire VMCLI ne lit pas l'entrée standard (stdin). Par conséquent, la redirection stdin n'est pas nécessaire.
- Exécution en arrière-plan : par défaut, l'utilitaire VMCLI s'exécute au premier plan. Utilisez les fonctions d'environnement de commande du système d'exploitation pour exécuter l'utilitaire en arrière-plan.

  Par exemple, sous Linux, le caractère perluète (&) suivant la commande convertit le programme en nouveau processus d'arrière-plan. Cette technique est utile dans les scripts, car elle permet au script de continuer après le démarrage d'un nouveau processus pour la commande VMCLI (autrement, le script se bloque jusqu'à la fin du programme VMCLI).

  Lorsque plusieurs sessions VMCLI démarrent, utilisez les fonctions du système d'exploitation pour lister et mettre fin aux processus.

15

Gestion de la carte SD vFlash

La carte SD vFlash est une carte Secure Digital (SD) qui se connecte dans le logement de carte SD vFlash du système. Vous pouvez utiliser une carte de 16 Go maximum. Après avoir inséré la carte, vous devez activer la fonctionnalité vFlash pour créer et gérer des partitions. vFlash est une fonction sous licence.

Si la carte n'est pas disponible dans le logement de carte SD vFlash du système, le message d'erreur suivant s'affiche dans l'interface Web iDRAC7 dans **Présentation générale → Serveur → vFlash**:

```
La carte SD n'est pas détectée. Insérez une carte SD de 256 Mo minimum.
```

REMARQUE : Veillez à insérer uniquement une carte SD compatible vFlash dans le logement de carte SD iDRAC7. Si vous insérez une carte non compatible, le message d'erreur suivant s'affiche lorsque vous initialisez la carte : *Erreur lors de l'initialisation de la carte SD.*

Les principales fonctions sont les suivantes :

- Fourniture d'un espace de stockage et émulation de périphériques USB.
- Création de 16 partitions maximum. Ces partitions, lorsqu'elles sont connectées au système, sont présentées comme lecteur de disquette, disque dur ou lecteur CD/DVD en fonction du mode d'émulation sélectionné.
- Création de partitions depuis les types de systèmes de fichiers compatibles. Prise en charge du format **.img** pour disquette, du format **.iso** pour CD/DVD et des formats **.iso** et **.img** pour les types d'émulation de disque dur.
- Création de périphériques USB amorçables.
- Démarrage uniquement depuis un périphérique USB émulé.

REMARQUE : Il peut arriver qu'une licence vFlash expire pendant une opération vFlash. Dans ce cas, l'opération en cours vFlash se termine normalement.

Configuration d'une carte SD vFlash

Avant de configurer vFlash, assurez-vous que la carte SD vFlash est installée sur le système. Pour plus d'informations sur l'installation et le retrait de la carte sur le système, voir le *Hardware Owner's Manual* (Manuel du propriétaire du matériel) du système sur le site **dell.com/support/manuals**.

REMARQUE : Vous devez disposer de l'autorisation de configuration d'iDRAC pour pouvoir activer ou désactiver vFlash et initialiser la carte.

Liens connexes

Affichage des propriétés d'une carte SD vFlash
Activation ou désactivation de la fonctionnalité vFlash
Initialisation d'une carte SD vFlash

Affichage des propriétés d'une carte SD vFlash

Après avoir activé la fonctionnalité vFlash, vous pouvez afficher les propriétés d'une carte SD avec l'interface Web iDRAC7 ou l'interface RACADM.

Affichage des propriétés d'une carte SD vFlash à l'aide de l'interface Web

Pour afficher les propriétés d'une carte SD vFlash, dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash**. La page **Propriétés de la carte SD** s'affiche. Pour plus d'informations sur les propriétés affichées, voir l'*Aide en ligne d'iDRAC7*.

Affichage des propriétés d'une carte SD vFlash à l'aide de l'interface RACADM

Pour afficher les propriétés de la carte SD vFlash à l'aide de la RACADM, utilisez l'une des opérations suivantes :

- Utilisez l'objet `cfgvFlashSD` avec la commande `getconfig`. Les propriétés en lecture seule suivantes s'affichent :
  - cfgVFlashSDSize
  - cfgVFlashSDLicensed
  - cfgVFlashSDAvailableSize
  - cfgVFlashSDHealth
  - cfgVFlashSDEnable
  - cfgVFlashSDWriteProtect
  - cfgVFlashSDInitialized
- Utilisez les objets suivants avec la commande `get` :
  - iDRAC.vflashsd.AvailableSize
  - iDRAC.vflashsd.Health
  - iDRAC.vflashsd.Licensed
  - iDRAC.vflashsd.Size
  - iDRAC.vflashsd.WriteProtect

Pour plus d'informations sur ces objets, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC*, disponible à l'adresse **dell.com/support/manuals** ou **dell.com/esmamanuals**.

Affichage des propriétés SD vFlash à l'aide de l'utilitaire de configuration d'iDRAC

Pour afficher les propriétés d'une carte SD vFlash, dans l'**Utilitaire de configuration d'iDRAC**, accédez à **Média vFlash**. La page **Paramètres iDRAC - Média vFlash** affiche les propriétés. Pour plus d'informations, sur les propriétés affichées, voir l'*Aide en ligne de l'Utilitaire de configuration d'iDRAC*.

Activation ou désactivation de la fonctionnalité vFlash

Vous devez activer la fonctionnalité vFlash pour pouvoir gérer les partitions.

Activation ou désactivation de la fonctionnalité vFlash à l'aide de l'interface Web

Pour activer ou désactiver la fonctionnalité vFlash :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** .
   La page **Propriétés de la carte SD** s'affiche.
2. Sélectionnez ou désélectionnez l'option **vFLASH activé** pour activer ou désactiver la fonctionnalité vFlash. Si une partition vFlash est connectée, vous ne pouvez pas désactiver vFlash et un message d'erreur s'affiche.

   REMARQUE : Si la fonctionnalité vFlash est désactivée, les propriétés de la carte SD ne s'affichent pas.
3. Cliquez sur **Appliquer**. La fonctionnalité vFlash est activée ou désactivée en fonction de la sélection.

Activation ou désactivation de la fonctionnalité vFlash à l'aide de RACADM

Pour activer ou désactiver la fonctionnalité vFlash à l'aide de la RACADM, utilisez l'une des opérations suivantes :

- Utilisation de la commande `config` :
  - Pour activer vFlash :
    `racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1`
  - Pour désactiver vFlash :
    `racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0`
- Avec la commande `set` :
  - Pour activer vFlash :
    `racadm set iDRAC.vflashsd.Enable 1`
  - Pour désactiver vFlash :
    `racadm set iDRAC.vflashsd.Enable 0`

REMARQUE : La commande RACADM fonctionne uniquement si une carte SD est présente. Dans le cas contraire, le message suivant s'affiche : *ERREUR : carte SD absente*.

Activation ou désactivation de la fonctionnalité vFlash à l'aide de l'utilitaire de configuration d'iDRAC

Pour activer ou désactiver la fonctionnalité vFlash :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **vFlash Media**.
   La page **Paramètres iDRAC-vFlash Media** s'affiche.
2. Sélectionnez **Activé** pour activer la fonctionnalité vFlash ou **Désactivé** pour la désactiver.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   La fonctionnalité vFlash est activée ou désactivée en fonction de la sélection.

Initialisation d'une carte SD vFlash

L'initialisation reformate la carte SD et configure les informations système vFlash sur la carte.

Initialisation d'une carte SD vFlash à l'aide de l'interface Web

Pour initialiser une vFlash SD :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale → Serveur → vFlash** .
   La page **Propriétés de la carte SD** s'affiche.
2. Activez **vFLASH** et cliquez sur **Initialiser**.
   Tout le contenu est supprimé de la carte et cette dernière est formatée avec les nouvelles informations système vFlash.
   Si une partition vFlash est connectée, l'opération d'initialisation échoue et un message d'erreur s'affiche.

Initialisation d'une carte SD vFlash à l'aide de l'interface RACADM

Pour initialiser la carte SD vFlash à l'aide de la RACADM, utilisez l'une des opérations suivantes :

- Avec la commande `vFlashSD` :
  `racadm vflashsd initialize`
- Avec la commande `set` :
  `racadm set iDRAC.vflashsd.Initialized 1`

Toutes les partitions existantes sont supprimées et la carte est reformatée.

Pour plus d'informations sur ces commandes, voir le manuel *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC*, disponible à l'adresse **dell.com/support/manuals** et **dell.com/esmmanuals**.

Initialisation d'une carte SD vFlash à l'aide de l'utilitaire de configuration d'iDRAC

Pour initialiser une carte SD vFlash à l'aide de l'utilitaire de configuration d'iDRAC :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Média vFlash**.
   La page **Paramètres iDRAC - Média vFlash** s'affiche.
2. Cliquez sur **Initialiser vFlash**.
3. Cliquez sur **Oui**. L'initialisation démarre.
4. Cliquez sur **Retour** et accédez à la page **Paramètres iDRAC - Média vFlash** pour afficher le message d'aboutissement.
   Tout le contenu existant est supprimé et la carte est reformatée avec les nouvelles informations système vFlash.

Obtention du dernier état à l'aide de l'interface RACADM

Pour obtenir l'état de la dernière commande d'initialisation envoyée à la carte SD vFlash :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez la commande `racadm vFlashsd status`
   L'état des commandes envoyées à la carte SD s'affiche.
3. Pour obtenir le dernier état de toutes les partitions vflash, exécutez la commande `racadm vflashpartition status -a`
4. Pour obtenir le dernier état d'une partition, exécutez la commande `racadm vflashpartition status -i (index)`

   REMARQUE : Si iDRAC7 est réinitialisé, l'état de la dernière opération de partition est perdue.

Gestion des partitions vFlash

Vous pouvez exécuter les opérations suivantes dans l'interface Web d'iDRAC7 ou RACADM :

REMARQUE : Un administrateur peut exécuter toutes les opérations sur les partitions vFlash. Autrement, vous devez disposer du privilège d'**Accès à Média Virtuel** pour pouvoir créer, supprimer, formater, connecter ou copier le contenu de la partition.

- Création d'une partition vide
- Création d'une partition à l'aide d'un fichier image
- Formatage d'une partition
- Affichage des partitions disponibles
- Modification d'une partition
- Connexion ou déconnexion de partitions
- Suppression de partitions existantes
- Téléchargement du contenu d'une partition
- Démarrage à partir d'une partition

REMARQUE : Si vous cliquez sur une option dans les pages vFlash lorsqu'une application, telle que WS-MAN, l'utilitaire de configuration d'iDRAC ou RACADM, utilise vFlash ou naviguez vers une autre page dans l'interface graphique, iDRAC7 affiche le message `vFlash est utilisé par un autre processus. Réessayez un peu plus tard`.

vFlash peut créer rapidement une partition lorsque aucune autre opération vFlash n'est en cours, telle que formatage, connexion de partitions, etc. Par conséquent, il est recommandé de créer toutes les partitions avant d'exécuter d'autres opérations de partition.

Création d'une partition vide

Une partition vide, lorsqu'elle est connectée au système, est similaire à un lecteur Flash USB vide. Vous pouvez créer des partitions vides sur la carte SD vFlash. Vous pouvez créer des partitions de type *Disquette* ou *Disque dur*. La partition de type CD est prise en charge uniquement lors de la création de partitions en utilisant des images.

Avant de créer une partition vide, vérifiez que :

- Vous disposez du privilège d'**Accès Média Virtuel**.
- La carte est initialisée.
- La carte n'est pas protégée contre l'écriture.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

Création d'une partition vide à l'aide de l'interface Web

Pour créer une partition vFlash vide :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Créer une partition vide**.

   La page **Créer une partition vide** s'affiche.
2. Entrez les informations nécessaires et cliquez sur **Appliquer**. Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.

   Une nouvelle partition vide non formatée est créée en lecture seule par défaut. Une page s'affiche pour indiquer le pourcentage d'avancement. Un message d'erreur s'affiche :

   - La carte est protégée contre l'écriture.
   - Le nom d'étiquette correspond à l'étiquette d'une partition existante.
   - Une valeur autre qu'un entier est entrée pour la taille de partition, la valeur dépasse l'espace disponible sur la carte ou la taille de partition est supérieure à 4 Go.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

Création d'une partition vide à l'aide de l'interface RACADM

Pour créer une partition vide de 20 Mo :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez la commande `racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20`

   Une partition vide de 20 Mo de format FAT16 est créée. Par défaut, une partition vide lisible et inscriptible est créée.

Création d'une partition à l'aide d'un fichier image

Vous pouvez créer une partition sur la carte SD vFlash en utilisant un fichier image (disponible dans le format **.img** ou **.iso**.) Les partitions sont des types d'émulations : disquette (**.img**), disque dur (**.img** ou **.iso**) ou CD (**.iso**). La taille de la partition créée est égale à la taille du fichier image.

Avant de créer une partition depuis un fichier image, vérifiez que :

- Vous disposez du privilège d'accès à Support Virtuel.
- La carte est initialisée.
- La carte n'est pas protégée contre l'écriture.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.
- Le type d'image et le type d'émulation correspondent.

  REMARQUE : L'image téléversée et le type d'émulation correspondent. Des problèmes apparaissent lorsque iDRAC7 émule un périphérique avec un type d'image incorrect. Par exemple, si la partition est créée en utilisant une image ISO et que le type d'émulation défini est Disque dur, le BIOS ne peut pas démarrer depuis cette image.
- La taille de l'image est inférieure ou égale à l'espace disponible sur la carte.
- La taille du fichier image est inférieure à 4 Go comme la taille de partition maximale est de 4 Go. Cependant, lors de la création d'une partition en utilisant un navigateur Web, le fichier image doit avoir une taille inférieure à 2 Go.

Création d'une partition à l'aide d'un fichier image et de l'interface Web

Pour créer une partition vFlash à l'aide d'un fichier image :

1. Dans l'interface iDRAC7, accédez à **Présentation générale → Serveur → vFlash → Créer depuis une image**.

   La page de **Créer une partition depuis un fichier image** s'affiche.
2. Entrez les informations appropriées et cliquez sur **Appliquer**. Pour plus d'informations sur les options, Voir l'*Aide en ligne d'iDRAC7*.

   Une partition est créée. Pour le type d'émulation CD, une partition en lecture seule est crée. Pour le type d'émulation Disquette ou Disque dur, une partition lisible et inscriptible est créée. Un message d'erreur s'affiche si :

   - La carte est protégée contre l'écriture.
   - Le nom d'étiquette correspond à l'étiquette d'une partition existante.
   - La taille du fichier image est supérieure à 4 Go ou excède l'espace disponible sur la carte.
   - Le fichier image n'existe pas ou son extension n'est ni .img ni .iso.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

Création d'une partition depuis un fichier image à l'aide de l'interface RACDAM

Pour créer une partition depuis un fichier image à l'aide de l'interface RACADM :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez la commande `racadm vflashpartition create –i 1 –o drive1 –e HDD –t image –l //monserveur/sharedfolder/foo.iso –u root –p monmotdepasse`

   Une partition est créée. Par défaut, elle est en lecture seule. Cette commande est sensible à la casse pour l'extension de nom de fichier image. Si l'extension du nom de fichier est en majuscules, par exemple FOO.ISO au lieu de FOO.iso, la commande renvoie une erreur de syntaxe.

   REMARQUE : Cette fonction n'est pas prise en charge dans l'interface RACADM locale.

   REMARQUE : La création d'une partition vFlash depuis un fichier image situé sur un partage de réseau IPv6 CFS ou NFS IPv6 n'est pas prise en charge.

Formatage d'une partition

Vous pouvez formater une partition existante sur la carte SD vFlash en fonction du type de système de fichiers. Les types de systèmes de fichiers compatibles sont EXT2, EXT3, FAT16 et FAT32. Vous pouvez formater des partitions de type Disque dur ou Disquette, mais pas CD. Vous ne pouvez pas formater des partitions en lecture seule.

Avant de créer une partition depuis un fichier image, vérifiez que :

- Vous disposez du privilège d'**accès Média Virtuel**.
- La carte est initialisée.
- La carte n'est pas protégée contre l'écriture.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

Pour formater la partition vFlash :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Formater**.
   La page **Formater la partition** s'affiche.
2. Saisissez les informations requises, puis cliquez sur **Appliquer**.
   Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC7*.
   Un message d'avertissement s'affiche pour indiquer que toutes les données de la partition seront effacées.
3. Cliquez sur **OK**.
   La partition sélectionnée est formatée en fonction du type de système de fichiers défini. Un message d'erreur s'affiche si :
   - La carte est protégée contre l'écriture.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

Affichage des partitions disponibles

Vérifiez que la fonctionnalité vFlash est activée pour pouvoir afficher la liste des partitions disponibles.

Affichage des partitions à l'aide de l'interface Web

Pour afficher les partitions vFlash, dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Gérer**. La page **Gérer des partitions** s'affiche avec la liste des partitions disponibles et les informations de chaque partition. Pour plus d'informations sur les partitions, voir l'*Aide en ligne d'iDRAC7*.

Affichage des partitions disponibles à l'aide de l'interface RACADM

Pour afficher les partitions disponibles et leurs propriétés en utilisant l'interface RACADM :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez les commandes suivantes :
   - Pour répertorier toutes les partitions existantes et leurs propriétés :
     ```
     racadm vflashpartition list
     ```
   - Pour obtenir l'état de fonctionnement de la partition 1 :
     ```
     racadm vflashpartition status -i 1
     ```
   - Pour obtenir l'état de toutes les partitions existantes :
     ```
     racadm vflashpartition status -a
     ```

     REMARQUE : L'option -a est valide uniquement avec l'option d'état.

Modification d'une partition

Vous pouvez convertir une partition en lecture seule en partition inscriptible et lisible et inversement. Avant de modifier la partition, vérifiez que :

- La fonctionnalité vFlash est activée.

- Vous disposez des privilèges d'**Accès Média Virtuel**.

REMARQUE : Par défaut, une partition en lecture seule est créée.

Modification d'une partition à l'aide de l'interface Web

Pour modifier des partitions :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Gérer**.
   La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Lecture seule** :
   - Cochez la case des partitions et cliquez sur **Appliquer** pour passer en lecture seule.
   - Cochez la case des partitions et cliquez sur **Appliquer** pour passer en lecture-écriture.
     Les partitions passent en lecture seule ou en lecture-écriture selon les sélections effectuées.

     REMARQUE : S'il s'agit d'une partition de type CD, l'état est Lecture seule. Vous ne pouvez pas remplacer l'état par lecture-écriture. Si la partition est connectée, la case est estompée.

Modification d'une partition en utilisant l'interface RACADM

Pour afficher les partitions disponibles et leurs propriétés sur la carte :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Procédez de l'une des manières suivantes :
   - Utilisation de la commande `config` pour modifier l'état de lecture/écriture de la partition :
     * Pour remplacer une partition en lecture seule par une partition en lecture-écriture :
       ```
       racadm config –g cfgvflashpartition –i 1 –o
       cfgvflashPartitionAccessType 1
       ```
     * Pour remplacer une partition en lecture-écriture par une partition en lecture seule :
       ```
       racadm config –g cfgvflashpartition –i 1 –o
       cfgvflashPartitionAccessType 0
       ```
   - Utilisation de la commande `set` pour modifier l'état de lecture/écriture de la partition :
     * Pour remplacer une partition en lecture seule par une partition en lecture-écriture :
       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 1
       ```
     * Pour remplacer une partition en lecture-écriture par une partition en lecture seule :
       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 0
       ```
   - Utilisation de la commande `set` pour définir le type d'émulation :
     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or
     CD-DVD>
     ```

Connexion et déconnexion de partitions

Lorsque vous connectez des partitions, elles sont accessibles au système d'exploitation et au BIOS comme périphériques de stockage de masse USB. Lorsque vous connectez plusieurs partitions en fonction de l'index affecté, elles sont répertoriées en ordre croissant dans le système d'exploitation et dans le menu de la séquence de démarrage BIOS.

Si vous déconnectez une partition, elle n'est pas accessible au système d'exploitation et elles ne figure pas dans le menu de la séquence de démarrage.

Lorsque vous connectez ou déconnectez une partition, le bus USB dan le système géré est réinitialisé. Ceci affecte les applications qui utilisent vFlash et déconnecte les sessions Média Virtuel iDRAC7.

Avant de connecter ou de déconnecter une partition :

- Activez la fonctionnalité vFlash.
- Vérifiez qu'aucune opération d'initialisation n'est en cours d'exécution sur la carte.
- Vérifiez que vous disposez des privilèges **d'accès Média Virtuel**.

Connexion et déconnexion de partitions à l'aide de l'interface Web

Pour connecter ou déconnecter des partitions :

1. Dans l'interface Web d'iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Gérer**.
   La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Connecté** :
   - Cochez la case de la ou des partitions et cliquez sur **Appliquer** pour connecter les partitions.
   - Désélectionnez la case de la ou des partitions et cliquez sur **Appliquer** pour déconnecter les partitions.
     Les partitions sont connectées ou déconnectées en fonction des sélections effectuées.

Connexion ou déconnexion de partitions à l'aide de l'interface RACADM

Pour connecter ou déconnecter des partitions :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Procédez de l'une des manières suivantes :
   - Utilisation de la commande `config` :
     * Pour connecter une partition :
       ```
       racadm config –g cfgvflashpartition –i 1 –o
       cfgvflashPartitionAttachState 1
       ```
     * Pour déconnecter une partition :
       ```
       racadm config –g cfgvflashpartition –i 1 –o
       cfgvflashPartitionAttachState 0
       ```
   - Avec la commande `set` :
     * Pour connecter une partition :
       ```
       racadm set iDRAC.vflashpartition. <index> .AttachState 1
       ```
     * Pour déconnecter une partition :
       ```
       racadm set iDRAC.vflashpartition. <index> .AttachState 0
       ```

Comportement du système d'exploitation pour les partitions connectées

Pour les systèmes d'exploitation Windows et Linux :

- Le système d'exploitation contrôle les lettres de lecteur et les affecte aux partitions connectées.
- Les partitions en lecture seule sont des lecteurs en lecture seule dans le système d'exploitation.
- Le système d'exploitation doit prendre en charge le système de fichiers d'une partition connectée pour qu'il puisse lire ou modifier le contenu de la partition. Par exemple, dans un environnement Windows, le système d'exploitation ne peut pas lire une partition de type EXT2 qui est native dans Linux. En outre, dans un environnement Linux, le système d'exploitation ne peut pas lire une partition de type NTFS qui est native dans Windows.

- L'étiquette de partition vFlash est différente du nom de volume du système de fichiers sur le lecteur émulé USB. Vous pouvez changer le nom de volume. Cette modification ne change pas le nom d'étiquette de partition stocké dans iDRAC7.

Suppression de partitions existantes

Avant de supprimer des partitions, vérifiez que :

- La fonctionnalité vFlash est activée.
- La carte n'est pas protégée contre l'écriture.
- La partition n'est pas connectée.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

Suppression de partitions existantes à l'aide de l'interface Web

Pour supprimer une partition existante :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Gérer**.
   La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Supprimer**, cliquez sur l'icône de suppression de la partition à supprimer.
   Un message s'affiche pour indiquer que l'action va supprimer définitivement la partition.
3. Cliquez sur **OK**.
   La partition est supprimée.

Suppression de partitions en utilisant l'interface RACADM

Pour supprimer des partitions :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez les commandes suivantes :
   - Pour supprimer une partition :
     ```
     racadm vflashpartition delete -i 1
     ```
   - Pour supprimer toutes les partitions, réinitialisez la carte SD vFlash.

Téléchargement du contenu d'une partition

Vous pouvez télécharger le contenu d'une partition vFlash dans le format **.img** ou **.iso** :

- sur le système géré (d'où iDRAC7 est exécuté) ;
- dans l'emplacement réseau mappé à une station de gestion.

Avant de télécharger le contenu de la partition, vérifiez que :

- Vous disposez des privilèges Média Virtuel.
- La fonctionnalité vFlash est activée.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.
- S'il s'agit d'une partition en lecture-écriture, elle ne doit pas être connectée.

Pour télécharger le contenu de la partition vFlash :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **vFlash** → **Télécharger**.
   La page **Télécharger la partition** s'affiche.
2. Dans le menu déroulant **Nom**, sélectionnez la partition à télécharger et cliquez sur **Télécharger**.

   REMARQUE : Toutes les partitions existantes (à l'exception des partitions connectées) s'affichent dans la liste. La première partition est la partition par défaut.
3. Spécifiez l'emplacement d'enregistrement du fichier.
   Le contenu de la partition sélectionnée est téléchargé vers l'emplacement spécifié.

   REMARQUE : Si vous définissez uniquement l'emplacement du dossier, le nom de la partition est utilisé comme nom de fichier avec l'extension **.iso** pour les types de partitions CD et Disque dur, et **.img** pour les types de partitions Disquette et Disque dur.

Démarrage à partir d'une partition

Vous pouvez définir une partition vFlash connectée en tant que périphérique de démarrage pour le démarrage suivant.

Avant de démarrer dans une partition,vérifiez que :

- La partition vFlash contient une image amorçable (de format **.img** ou **.iso**) pour démarrer le périphérique.
- La fonctionnalité vFlash est activée.
- Vous disposez des privilèges d'accès à Média Virtuel.

Démarrage depuis une partition à l'aide de l'interface Web

Pour définir la partition vFlash comme premier périphérique de démarrage, voir Définition du premier périphérique de démarrage.

REMARQUE : Si la ou les partitions vFlash connectées ne figurent pas dans le menu déroulant **Premier périphérique de démarrage**, vérifiez que vous disposez de la dernière version du BIOS.

Démarrage dans une partition à l'aide de l'interface RACADM

Pour définir une partition vFlash comme premier périphérique de démarrage, utilisez `cfgServerInfo`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur **dell.com/support/manuals**.

REMARQUE : Lorsque vous exécutez la commande, l'étiquette de partition vFlash est définie automatiquement pour un seul démarrage ; `cfgserverBootOnce` est affecté de la valeur `1`. Dans ce cas, le périphérique démarre dans la partition une seule fois et il ne reste pas le premier périphérique de la séquence de démarrage.

16

Utilisation de SMCLP

La spécification SMCLP (Server Management Command Line Protocol) permet de gérer les systèmes CLI. Elle définit un protocole pour les commandes de gestion envoyées dans des flux orientés caractère standard. Ce protocole accède à un Gestionnaire CIMOM (Common Information Model Object Manager) en utilisant un groupe de commandes manuelles. SMCLP est un sous-composant du projet SMASH DMTF (Distributed Management Task Force) pour rationaliser la gestion des systèmes sur plusieurs plates-formes. La spécification SMCLP, et la spécification Managed Element Addressing Specification et de nombreux profils dans les spécifications de mappage SMCLP, décrit les verbes et les cibles standard pour les exécutions de tâches de gestion.

REMARQUE : Elle suppose que vous connaissez le projet SMASH (Systems Management Architecture for Server Hardware) et les spécifications SMWG SMCLP.

SM-CLP est un sous-composant du projet SMASH DMTF (Distributed Management Task Force) pour rationaliser la gestion des serveurs sur plusieurs plate-formes. La spécification SM-CLP, et la spécification MEAS (Managed Element Addressing Specification) et les nombreux profils dans les spécifications SM-CLP, décrit les verbes et les cibles standard des exécutions de tâches de gestion.

SMCLP est hébergé depuis le micrologiciel du contrôleur iDRAC7 et prend en charge les interfaces Telnet, SSH et série. L'interface SMCLP iDRAC7 repose sur la spécification SMCLP 1.0 fournie par l'organisation DMTF.

REMARQUE : Des informations sur les profils, les extensions et les MOF sont disponibles sur **delltechcenter.com** et toutes les informations DMTF sont disponibles sur **dmtf.org/standards/profiles/**.

Les commandes SM-CLP mettent en œuvre un sous-ensemble de commandes RACADM. Les commandes sont pratiques pour le scriptage, puisque vous pouvez les exécuter depuis une ligne de commande de station de gestion. Vous pouvez extraire la sortie des commandes dans des formats bien définis, notamment XML, ce qui facilite le scriptage et l'intégration aux outils de génération de rapport et de gestion.

Fonctions de gestion de système à l'aide de SMCLP

SMCLP iDRAC7 permet de :

- Gérer l'alimentation du serveur : mise sous tension, arrêt ou redémarrage du système
- Gérer le journal des événements système (SEL) : affichage ou effacement des enregistrements du journal SEL
- Gérer le compte d'utilisateur iDRAC7
- Afficher les propriétés du système

Exécution des commandes SMCLP

Vous pouvez exécuter les commandes SMCLP en utilisant une interface SSH ou Telnet. Ouvrez une interface SSH ou Telnet et ouvrez une session dans iDRAC7 comme administrateur. L'invite SMCLP (admin ->) s'affiche.

Invites SMCLP :

- serveurs lames yx1x, utilisez `–$`.
- serveurs en rack et de type tour yx1x, utilisez `admin->`.

- serveurs lames, en rack et de type tour yx2x, utilisez `admin->`.

, où y est un caractère alphanumérique, tel que M (pour serveurs lames), R (pour serveurs en rack) et T (pour les serveurs de type tour), et x est un nombre. Ceci indique la génération des serveurs Dell PowerEdge.

REMARQUE : Les scripts qui utilisent `–$` peuvent utiliser ces données pour les systèmes yx1x, mais à partir des systèmes yx2x un script avec `admin->` peut être utilisé pour les serveurs lames, en rack et de type tour.

Syntaxe SMCLP iDRAC7

SMCLPP iDRAC7 utilise le concept de verbe et de cible pour fournir des fonctions de gestion de systèmes via l'interface CLI. Un verbe indique l'opération à exécuter et une cible détermine l'entité (ou l'objet) qui exécute l'opération.

Syntaxe de ligne de commande SMCLP :

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

Le tableau suivant répertorie les verbes et leur définition.

Tableau 28. Verbes SMCLP

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

Le tableau suivant répertorie les cibles.

Tableau 29. Cibles SMCLP

Cible	Définitions
`admin1`	domaine admin
`admin1/profiles1`	Profils enregistrés dans iDRAC7
`admin1/hdwr1`	Matériel
`admin1/system1`	Cible du système géré
`admin1/system1/capabilities1`	Fonctions de collecte SMASH du système géré
`admin1/system1/capabilities1/pwrcap1`	Fonctions d'utilisation de l'alimentation du système géré
`admin1/system1/capabilities1/elecap1`	Fonctions de cible du système géré

Cible	Définitions
admin1/system1/logs1	Cible des collectes du journal d'enregistrements
admin1/system1/logs1/log1	Entrée d'enregistrement du journal des événements système (SEL)
admin1/system1/logs1/log1	Instance d'enregistrement SEL individuelle sur le système géré
admin1/system1/settings1	Paramètres de collecte SMASH du système géré
admin1/system1/capacities1	Collecte SMASH des capacités du système géré
admin1/system1/consoles1	Collecte SMASH des consoles du système géré
admin1/system1/sp1	Processeur de service
admin1/system1/sp1/timesvc1	Service de temps du processeur de service
admin1/system1/sp1/capabilities1	Collecte SMASH des capacités du processeur de service
admin1/system1/sp1/capabilities1/ clpcap1	Fonctions de service CLP
admin1/system1/sp1/capabilities1/ pwrmgtcap1	Fonctions de service de gestion de l'état de l'alimentation sur le système
admin1/system1/sp1/capabilities1/ acctmgtcap*	Fonctions de service de gestion de comptes
admin1/system1/sp1/capabilities1/ rolemgtcap*	Fonctions de gestion basées sur les rôles locaux
admin1/system1/sp1/capabilities/ PwrutilmgtCap1	Fonctions de gestion de l'utilisation de l'alimentation
admin1/system1/sp1/capabilities1/ elecap1	Fonctions d'authentification
admin1/system1/sp1/settings1	Collecte des paramètres du processeur de service
admin1/system1/sp1/settings1/ clpsetting1	Données des paramètres de service CLP
admin1/system1/sp1/clpsvc1	Service de protocole de service CLP
admin1/system1/sp1/clpsvc1/clpendpt*	Terminaison de protocole de service CLP
admin1/system1/sp1/clpsvc1/tcpendpt*	Terminaison TCP de protocole de service CLP
admin1/system1/sp1/jobq1	File d'attente des tâches du protocole de service CLP
admin1/system1/sp1/jobq1/job*	Tâche du protocole de service CLP
admin1/system1/sp1/pwrmgtsvc1	Service de gestion de l'état de l'alimentation
admin1/system1/sp1/account1-16	Compte d'utilisateur local

Cible	Définitions
admin1/sysetm1/sp1/account1-16/identity1	Compte d'identité d'utilisateur local
admin1/sysetm1/sp1/account1-16/identity2	Compte d'identité IPMI (LAN)
admin1/sysetm1/sp1/account1-16/identity3	Compte d'identité IPMI (série)
admin1/sysetm1/sp1/account1-16/identity4	Compte d'identité CLP
admin1/system1/sp1/acctsvc1	Service de gestion de compte d'utilisateur local
admin1/system1/sp1/acctsvc2	Service de gestion de compte IPMI
admin1/system1/sp1/acctsvc3	Service de gestion de compte CLP
admin1/system1/sp1/rolesvc1	Service d'autorisation basée sur des rôles (RBA) locaux
admin1/system1/sp1/rolesvc1/Role1-16	Rôle local
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	Privilège de rôle local
admin1/system1/sp1/rolesvc2	Service RBA IPMI
admin1/system1/sp1/rolesvc2/Role1-3	Rôle IPMI
admin1/system1/sp1/rolesvc2/Role4	Rôle Série sur LAN (SOL) IPMI
admin1/system1/sp1/rolesvc3	Service RBA CLP
admin1/system1/sp1/rolesvc3/Role1-3	Rôle CLP
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	Privilège de rôle CLP

Liens connexes

Exécution des commandes SMCLP
Exemples d'utilisation

Navigation dans l'espace d'adressage MAP

Les objets qui peuvent être gérés avec SM-CLP sont représentés par des cibles organisées dans un espace hiérarchique appelé espace d'adressage MAP (Manageability Access Point). Un chemin d'adressage définit le chemin de la racine de l'espace d'adressage vers un objet dans l'espace d'adresse.

La cible racine est représentée par une barre oblique (/) ou une barre oblique inverse (\). Il s'agit du point de départ par défaut lorsque vous ouvrez une session dans iDRAC7. Accédez à la racine en utilisant le verbe `cd`.

REMARQUE : La barre oblique (/) et la barre oblique inverse (\) sont permutables dans les chemins d'adressage SM-CLP. Toutefois, une barre oblique inverse à la fin d'une ligne de commande continue la commande sur la ligne suivante et elle est ignorée lorsque la commande est analysée.

Par exemple, pour accéder au troisième enregistrement du journal des événements système (SEL), entrez la commande suivante :

```
->cd /admin1/system1/logs1/log1/record3
```

Entrez le verbe `cd` sans cible pour rechercher l'emplacement en cours dans l'espace d'adressage. Les abréviations `..` et `.` fonctionnent comme dans Windows et Linux : `...` fait référence au niveau parent et `.`, au niveau en cours.

Utilisation du verbe Show

Pour en savoir plus sur une cible, utilisez le verbe `show`. Ce verbe affiche les propriétés de la cible, des sous-cibles, des associations et la liste des verbes SM-CLP autorisés dans l'emplacement.

Utilisation de l'option -display

L'option `show -display` permet de limiter la sortie de la commande à une ou plusieurs propriétés, cibles, associations et un ou plusieurs verbes. Par exemple, pour afficher uniquement les propriétés et les cibles dans 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/sp1/account1
```

Si vous souhaitez uniquement afficher une propriété, vous pouvez omettre les parenthèses.

Utilisation de l'option -level

L'option `show -level` exécute `show` sur les niveaux supplémentaires sous la cible définie. Pour afficher toutes les cibles et les propriétés dans 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**, **keyword** et **clpxml**.

Le format par défaut **text** est le plus lisible. Le format **clpcsv** est un format de valeurs séparées par une virgule à charger dans un tableur. Le format **keyword** génère des informations dans une liste de paires keyword=value avec une paire sur chaque ligne. Le format **clpxml** est un document XML qui contient un élément XML de **réponse**. DMTF a défini les formats **clpcsv** et **clpxml** et leurs spécifications sont disponibles sur le site Web DMTF, **dmtf.org**.

L'exemple suivant montre comment générer le contenu du journal SEL dans le format XML :

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Exemples d'utilisation

Cette section fournit des scénarios de cas d'utilisation pour SMCLP:

- Gestion de l'alimentation du serveur
- Gestion du journal SEL
- Navigation dans la cible MAP

Gestion de l'alimentation du serveur

Les exemples suivants expliquent comment utiliser SMCLP pour exécuter des opérations de gestion de l'alimentation sur un système géré.

Tapez les commandes suivantes dans l'invite de commande SMCLP :

- Pour arrêter le serveur :
  ```
  stop /system1
  ```
  Le message suivant s'affiche :
  ```
  Le système 1 a été correctement arrêté.
  ```
- Pour démarrer le serveur :
  ```
  start /system1
  ```
  Le message suivant s'affiche :
  ```
  Le système a été correctement démarré.
  ```
- Pour redémarrer le serveur :
  ```
  reset /system1
  ```
  Le message suivant s'affiche :
  ```
  Le système 1 a été correctement réinitialisé.
  ```

Gestion du journal SEL

Les exemples suivants expliquent comment utiliser le protocole SMCLP pour exécuter des opérations SEL sur le système géré. Tapez les commandes suivantes dans l'invite de commande SMCLP :

- Pour afficher le journal SEL :
  ```
  show/system1/logs1/log1
  ```
  La sortie suivante s'affiche :
  ```
  /system1/logs1/log1
  Targets:
  Record1
  Record2
  Record3
  Record4
  Record5
  Properties:
  InstanceID = IPMI:BMC1 SEL Log
  MaxNumberOfRecords = 512
  CurrentNumberOfRecords = 5
  Name = IPMI SEL
  EnabledState = 2
  OperationalState = 2
  HealthState = 2
  Caption = IPMI SEL
  Description = IPMI SEL
  ElementName = IPMI SEL
  Commands:
  cd
  show
  help
  exit
  version
  ```

- Pour afficher l'enregistrement SEL :
  ```
  show/system1/logs1/log1
  ```
  La sortie suivante s'affiche :
  ```
  /system1/logs1/log1/record4
  Properties:
  LogCreationClassName= CIM_RecordLog
  CreationClassName= CIM_LogRecord
  LogName= IPMI SEL
  RecordID= 1
  MessageTimeStamp= 20050620100512,000000-000
  Description= FAN 7 RPM: fan sensor, detected a failure
  ElementName= IPMI SEL Record
  Commands:
  cd
  show
  help
  exit
  version
  ```
- Pour effacer le journal SEL :
  ```
  delete /system1/logs1/log1/record*
  ```
  La sortie suivante s'affiche :
  ```
  All records deleted successfully (Tous les enregistrements ont été
  correctement supprimés).
  ```

Navigation dans la cible MAP

Les exemples suivants montrent comment utiliser le verbe cd pour naviguer dans MAP. Dans tous les exemples, la cible par défaut initiale est supposée être /.

Tapez les commandes suivantes dans l'invite de commande SMCLP :

- Pour accéder à la cible système et redémarrer :
  cd system1 reset. La cible par défaut actuelle est /.
- Pour accéder à la cible SEL et afficher les enregistrements du journal :
  ```
  cd system1
  cd logs1/log1
  show
  ```
- Pour afficher la cible en cours :
  type `cd .`
- Pour monter d'un niveau :
  type `cd ..`
- Pour quitter :
  ```
  exit
  ```

17

Utilisation du module de service iDRAC

La surveillance iDRAC dépend actuellement de OpenManage Server Administrator pour fournir des informations sur l'hôte, telles que le système d'exploitation et le nom d'hôte. Le module de service iDRAC est une application logicielle qui est recommandée sur le serveur (elle n'est pas installée par défaut). Elle vient compléter l'iDRAC en fournissant des données de surveillance du système d'exploitation. Elle ne possède pas d'interface mais complète l'iDRAC en fournissant des données supplémentaires pour fonctionner avec les interfaces iDRAC telles que l'interface Web, RACADM et WSMAN. Vous pouvez configurer les fonctionnalités surveillées par le module de service iDRAC pour contrôler le processeur et la mémoire utilisée sur le système d'exploitation du serveur.

REMARQUE : Vous pouvez utiliser le module de service iDRAC uniquement si vous avez installé une licence de contrôleur iDRAC Express ou iDRAC Enterprise.

Avant d'utiliser le module de service iDRAC, assurez-vous que :

- Vous disposez de privilèges de connexion, de configuration et de contrôle de serveur dans iDRAC pour activer ou désactiver les fonctions du module de service iDRAC.
- la fonction de transfert du SE à iDRAC est activée par l'intermédiaire de l'USB interne dans l'iDRAC7.

  REMARQUE :

  – Lorsque le module de service iDRAC s'exécute pour la première fois, il active par défaut la connexion directe entre le système d'exploitation et l'iDRAC dans iDRAC. Si vous désactivez cette fonction après l'installation du module de service iDRAC, vous devez l'activer manuellement dans l'iDRAC.

  – Si la connexion directe entre le système d'exploitation et l'iDRAC est activée via le LOM dans iDRAC7, vous ne pouvez pas utiliser le module de service iDRAC.

Installation du module de service iDRAC

Vous pouvez télécharger et installer le module iDRAC depuis le site **dell.com/support**. Vous devez avoir des privilèges d'administrateur sur le système d'exploitation du serveur pour installer le module de service iDRAC. Pour plus d'informations sur l'installation, consultez le *Guide d'installation du module de service iDRAC* disponible à l'adresse **dell.com/support/manuals**.

Fonctionnalités de surveillance du module de service iDRAC

Le module du service iDRAC fournit les fonctionnalités de surveillance suivantes :

- Informations sur le système d'exploitation (SE)
- Réplication des journaux Lifecycle Controller dans les journaux du système d'exploitation.
- Options de récupération automatique du système

Informations sur le système d'exploitation

OpenManage Server Administrator partage actuellement les informations sur le système d'exploitation et le nom d'hôte avec l'iDRAC. Le module de service iDRAC fournit les mêmes informations telles que le nom du système d'exploitation, la version du système d'exploitation et le nom de domaine complet (FQDN) avec iDRAC. Par défaut, cette fonctionnalité de

surveillance est activée. Elle n'est pas désactivée si OpenManage Server Administrator est installé sur le système d'exploitation hôte.

Réplication des journaux Lifecycle dans ceux du SE

Vous pouvez répliquer les journaux Lifecycle Controller sur les journaux du système d'exploitation à partir de l'heure à laquelle la fonction est activée dans l'iDRAC. Ce cas est similaire à la réplication du journal des événements système (SEL) effectuée par OpenManage Server Administrator. Les événements dont l'option **Journal du système d'exploitation** est sélectionnée comme cible (dans la page **Alertes** ou dans les interfaces équivalentes RACADM ou WSMAN) sont répliqués dans le journal du système d'exploitation à l'aide du module de service iDRAC. Le jeu par défaut des journaux à inclure dans les journaux du système d'exploitation est le même que celui qui est configuré pour les alertes ou interruptions SNMP.

Le module de service iDRAC journalise également les événements qui se sont produits lorsque le système d'exploitation ne fonctionne pas. La journalisation du système d'exploitation effectuée par le module de service iDRAC suit les normes de journalisation système IETF pour les systèmes d'exploitation basés sur Linux.

Si OpenManage Server Administrator est installé, cette fonctionnalité de surveillance est désactivée pour éviter les doublons d'entrées du journal SEL dans le journal du système d'exploitation.

Options de récupération automatique du système

Vous pouvez effectuer des opérations de récupération automatique du système, telles que le redémarrage, le cycle d'alimentation, ou la mise hors tension du serveur après une période spécifique. Cette fonctionnalité est activée uniquement si l'horloge de surveillance du système d'exploitation est désactivée. Si OpenManage Server Administrator est installé, cette fonctionnalité de surveillance est désactivée pour éviter toute duplication des horloges de surveillance.

Coexistence d'OpenManage Server Administrator et du module de service iDRAC

Dans un système, OpenManage Server Administrator et le module de service iDRAC peuvent tous deux coexister et continuer de fonctionner correctement et de manière indépendante.

Si vous avez activé les fonctions de surveillance iDRAC au cours de l'installation du module de service, une fois l'installation terminée, si le module de service iDRAC détecte la présence d'OpenManage Server Administrator, il désactive l'ensemble de fonctionnalités de surveillance qui se chevauchent. Si OpenManage Server Administrator est en cours d'exécution, le module de service iDRAC désactive les fonctionnalités de surveillance qui se chevauchent après avoir ouvert une session sur le système d'exploitation et l'iDRAC.

Lorsque vous réactivez ces fonctionnalités de surveillance via les interfaces iDRAC ultérieurement, les mêmes opérations sont effectuées et les fonctionnalités sont activées selon qu'OpenManage Server Administrator est en cours d'exécution ou non.

Utilisation du module de service iDRAC à partir de l'interface Web de l'iDRAC

Pour utiliser le module de service iDRAC à partir de l'interface Web iDRAC :

1. Accédez à **Présentation générale** → **Serveur** → **Module de service**.
   La page de **configuration du module de service iDRAC** s'affiche.
2. Vous pouvez afficher ce qui suit :
   - La version du module de service iDRAC installée sur le système d'exploitation hôte
   - L'état de connexion du module de service iDRAC à l'iDRAC.
3. Pour utiliser des fonctions de surveillance hors bande, sélectionnez une ou plusieurs des options suivantes :
   - **Informations sur le système d'exploitation** : affiche les informations sur le système d'exploitation.
   - **Répliquer le journal Lifecycle dans le journal du système d'exploitation** : inclut les journaux Lifecycle Controller aux journaux du système d'exploitation. Cette option est désactivée si OpenManage Server Administrator est installé sur le système.
   - **Action de récupération de système automatique** : exécution des opérations de récupération automatique sur le système après un certain temps (en secondes) :
     * **Redémarrer**
     * **Arrêter le système**
     * **Exécuter un cycle d'alimentation sur le système**

     Cette option est désactivée si OpenManage Server Administrator est installé sur le système.

Utilisation du module de service iDRAC à l'aide de la RACADM

Pour utiliser le module de service iDRAC à partir de la RACADM, utilisez les objets du groupe **ServiceModule**. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC* disponible à l'adresse **dell.com/support/manuals**.

18

Déploiement de systèmes d'exploitation

Vous pouvez utiliser n'importe quel utilitaire pour déployer des systèmes d'exploitation sur les systèmes gérés :

- Interface de ligne de commande CLI Média Virtuel
- Console Média Virtuel
- Partage de fichier à distance

Liens connexes

Déploiement de votre système d'exploitation en utilisant VMCLI
Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance
Déploiement d'un système d'exploitation à l'aide de Média Virtuel

Déploiement de votre système d'exploitation en utilisant VMCLI

Avant de déployer le système d'exploitation en utilisant le script vmdeploy vérifiez que :

- L'utilitaire VMCLI est installé sur la station de gestion.
- Les privilèges de **Configuration** d'**Utilisateur** et d'**Accès à Média Virtuel** d'iDRAC7 sont activés pour l'utilisateur.
- L'utilitaire IPMItool est installé sur la station de gestion.

  REMARQUE : IPMItool ne fonctionne pas si IPv6 est configuré sur le système géré ou la station de gestion.
- iDRAC7 est configuré sur les systèmes distants cibles.
- Le système peut démarrer depuis le fichier image.
- IPMI sur LAN est activé dans iDRAC7.
- Le partage de réseau contient les pilotes et le fichier image amorçable du système d'exploitation dans le format standard **.img** ou **.iso**.

  REMARQUE : Lors de la création du fichier image, suivez les procédures d'installation réseau normales et rendez l'image de déploiement accessible en lecture seule pour que chaque système cible démarre et exécute la même procédure de déploiement.
- L'état de Média Virtuel est Connexion.
- Le script **vmdeploy** est installé sur la station de gestion. Reportez-vous à cet exemple de script vmdeploy fourni avec VMCLI. Le script décrit le déploiement du système d'exploitation sur des systèmes distants dans le réseau. Il utilise VMCLI et IPMItool en interne.

  REMARQUE : Le script **vmdeploy** dépend de fichiers de support dans le répertoire au cours de l'installation. Pour utiliser le script depuis un autre répertoire, copiez tous les fichiers avec le répertoire. Si l'utilitaire IPMItool n'est pas installé, copiez l'utilitaire avec les autres fichiers.

Pour déployer le système d'exploitation sur les systèmes distants cibles :

1. Listez les adresses IPv4 iDRAC7 des systèmes distants cibles dans le fichier texte **ip.txt**. Listez une adresse IPv4 par ligne.
2. Insérez un CD ou un DVD de système d'exploitation amorçable dans le lecteur de la station de gestion.

3. Ouvrez une invite de commande avec les privilèges d'administrateur et exécutez le script **vmdeploy** :

```
vmdeploy.bat -r <iDRAC7-adresse IP ou fichier> -u <iDRAC7-utilisateur> -p
<iDRAC7-utilisateur-passwd> [ -f {<image-lecteur de disquette> | <nom
périphérique>} | -c { <nom périphérique>|<fichier image>} ] [-i <ID
périphérique>]
```

REMARQUE : Comme IPv6 ne prend pas en charge l'outil IPMI, vmdeploy ne prend pas en charge IPv6.

REMARQUE : Le script vmdeploy traite l'option `-r` un peu différemment par rapport à l'option `vmcli -r`. Si l'argument de l'option `-r` est le nom d'un fichier existant, le script lit les adresses iDRAC7 IPv4 ou IPv6 depuis le fichier défini et exécute l'utilitaire une fois pour chaque ligne. Si l'argument de l'option `-r` n'est pas un nom de fichier, il doit lire une seule adresse iDRAC7. Dans ce cas, l'option-**r** fonctionne, comme indiqué pour l'utilitaire VMCLI.

Le tableau suivant répertorie les paramètres de la commande vmdeploy.

Tableau 30. Paramètres de la commande vmdeploy

Paramètre	Description
`<iDRAC7 utilisateur>`	Nom d'utilisateur iDRAC7. Il doit avoir les attributs suivants : – Nom d'utilisateur valide – Droit d'utilisateur Média Virtuel iDRAC7 Si l'authentification iDRAC7 échoue, un message d'erreur s'affiche et la commande se termine.
`<iDRAC7-adresse IP| fichier>`	Adresse IP iDRAC7 du fichier contenant l'adresse IP d'iDRAC7 IP.
`<iDRAC7-mot de passe utilisateur>` ou `<iDRAC7-passwd>`	Mot de passe de l'utilisateur iDRAC7. Si l'authentification iDRAC7 échoue, un message d'erreur s'affiche et la commande se termine.
`-c {<nom de périphérique> | <fichier image>}`	Chemin d'une image ISO9660 du CD ou du DVD d'installation du système d'exploitation.
`<lecteur de disquette>`	Chemin du périphérique contenant le CD, le DVD ou la disquette du système d'exploitation.
`<image de disquette>`	Chemin d'une image de disquette valide.
`<ID de périphérique>`	ID du périphérique à démarrage unique.

Liens connexes

Configuration de Média Virtuel
Configuration d'iDRAC7

Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance

Avant de déployer le système d'exploitation à l'aide de RFS (Remote File Share - Partage de fichiers à distance), vérifiez que :

- Les privilèges de **Configuration Utilisateur** et d'**Accès au média virtuel** d'iDRAC7 sont activés pour l'utilisateur.
- Le partage de réseau contient des pilotes et un fichier d'image amorçable du système d'exploitation dans un format standard, tel que **.img** ou **.iso**.

REMARQUE : Lors de la création du fichier image, suivez les procédures d'installation réseau standard et marquez l'image de déploiement comme étant en lecture seule pour que chaque système cible démarre et exécute la même procédure de déploiement.

Pour déployer un système d'exploitation à l'aide de RFS :

1. À l'aide de RFS, montez le fichier d'image ISO ou IMG sur le système géré par l'intermédiaire de NFS ou CIFS (Common Internet File Sharing).
2. Allez dans **Présentation** → **Configuration** → **Premier périphérique de démarrage** .
3. Définissez **Partage de fichier à distance** pour la séquence de démarrage dans la liste déroulante **Premier périphérique de démarrage**.
4. Sélectionnez l'option **Démarrage unique** pour permettre au système géré de démarrer en utilisant le fichier image pour la prochaine instance uniquement.
5. Cliquez sur **Appliquer**.
6. Redémarrez le système géré et suivez les instructions qui s'affichent pour effectuer le déploiement.

Liens connexes

Gestion du partage de fichier à distance
Définition du premier périphérique de démarrage

Gestion du partage de fichier à distance

Avec la fonction de partage de fichier à distance (RFS), vous pouvez définir un fichier image ISO ou IMG situé sur un partage de réseau et le rendre accessible au système d'exploitation du serveur géré comme lecteur virtuel en le montant comme CD ou DVD à l'aide de NFS ou CIFS. Cette fonction est disponible sous licence.

REMARQUE : Les adresses IPv4 sont prises en charge pour CIFS et NFS. Les adresses IPv6 sont prises en charge uniquement pour CIFS.

Le partage de fichier à distance prend en charge uniquement les formats de fichier d'image **.img** et **iso**. Un fichier **.img** est redirigé comme disquette virtuelle, et un fichier **.iso** est redirigé comme CD-ROM virtuel.

Vous devez posséder les privilèges Média Virtuel pour pouvoir effectuer un montage de RFS.

REMARQUE : Si ESXi fonctionne sur un système géré et que vous montez une image de disquette (**.img**) en utilisant le partage de fichier à distance, l'image de disquette virtuelle n'est pas accessible au système d'exploitation ESXi.

RFS et les fonctionnalités de média virtuel sont mutuellement exclusifs.

- Si le client média virtuel n'a pas été lancé, et que vous tentez d'établir une connexion RFS, celle-ci est établie et l'image distante devient accessible au système d'exploitation hôte.
- Si le client média virtuel a été lancé et que vous tentez d'établir une connexion RFS, le message d'erreur suivant s'affiche :

  Le Média virtuel est détaché ou redirigé pour le lecteur virtuel sélectionné.

L'état de connexion de RFS est disponible dans le journal iDRAC7. Une fois connecté, un lecteur virtuel monté avec RFS ne se déconnecte pas, même si vous fermez la session dans iDRAC7. La connexion RFS est fermée si iDRAC7 est réinitialisé ou que la connexion réseau est perdue. L'interface Web et les options de commande sont également disponibles dans CMC et iDRAC7 pour fermer la connexion RFS. La connexion RFS depuis CMC remplace toujours un montage RFS existant dans iDRAC7.

REMARQUE : La fonction vFlash iDRAC7 et RFS ne sont pas associés.

Si vous mettez à jour le micrologiciel iDRAC de la version 1.30.30 à 1.50.50 alors qu'il existe une connexion RFS active et que le mode de connexion du média virtuel est défini sur **Connecter** ou **Auto-connecter**, l'iDRAC tente de rétablir la connexion RFS après la mise à niveau du micrologiciel et le redémarrage de l'iDRAC.

Si vous mettez à jour le micrologiciel iDRAC de la version 1.30.30 à 1.50.50 alors qu'il existe une connexion RFS active et que le mode de connexion du média virtuel est défini sur **Déconnecter**, l'iDRAC ne tente pas de rétablir la connexion RFS après la mise à niveau du micrologiciel et le redémarrage de l'iDRAC.

Configuration du partage de fichier à distance en utilisant l'interface Web

Pour activer le partage de fichier à distance :

1. Dans l'interface Web iDRAC7, accédez à **Présentation** → **Serveur** → **Média connecté**.
   La page **Média connecté** s'affiche.
2. Sous **Médias connectés**, sélectionnez **Connecter** ou **Connecter automatiquement**.
3. Sous **Partage de fichier à distance**, spécifiez le chemin d'accès au fichier image, le nom de domaine, le nom d'utilisateur et le mot de passe. Pour en savoir plus sur les champs, voir l'*aide en ligne iDRAC7*.
   Exemple de chemin d'accès à un fichier d'image :
   - CIFS : //<adresse IP pour connexion au système de fichiers CIFS>/<chemin de fichier>/<nom de l'image>
   - NFS : <adresse IP pour connexion au système de fichiers NFS>:/<chemin d'accès au fichier>/<nom de l'image>

   REMARQUE : Les caractères '/' ou '\' peuvent être utilisés pour le chemin d'accès au fichier.

   CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.

   Si vous utilisez le partage NFS, assurez-vous d'indiquer le <chemin d'accès au fichier> et le <nom de l'image> exacts car ils sont sensibles à la casse.
4. Cliquez sur **Appliquer**, puis sur **Connecter**.
   Une fois la connexion établie, l'**État de la connexion** indique **Connecté**.

   REMARQUE : Même si vous avez configuré le partage de fichier à distance, l'interface utilisateur n'affiche pas les informations d'identification de l'utilisateur pour des raisons de sécurité.

   Pour les distributions Linux, cette fonction peut nécessiter une commande de montage manuel au niveau d'exécution init 3. La syntaxe de la commande est :

   ```
   mount /dev/OS_specific_device / user_defined_mount_point
   ```

   , où `user_defined_mount_point` correspond à un répertoire que vous choisissez d'utiliser comme pour n'importe quelle commande de montage.

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

   Pour SLES, le périphérique CD est `/dev/sr0` et le périphérique de disquette est /dev/sdc. Pour utiliser le périphérique correct (pour SLES ou RHEL), lorsque vous vous connectez le périphérique virtuel, vous devez exécuter immédiatement la commande sur Linux :

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

   La commande affiche le texte qui identifie le périphérique (SCSI sdc, par exemple). Cette procédure s'applique également à Média Virtuel lorsque vous utilisez des distributions au niveau d'exécution init 3. Par défaut, le média virtuel n'est pas monté automatiquement dans init 3.

Configuration du partage de fichier à distance à l'aide de l'interface RACADM

Pour configurer le partage de fichier à distance en utilisant l'interface RACADM, lancez la commande :

```
racadm remoteimage
racadm remoteimage <options>
```

Les options sont les suivantes :

`-c` : connecter une image

`-d` : déconnecter une image

`-u` <nom d'utilisateur> : nom d'utilisateur permettant d'accéder au partage de réseau

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

`-l` <image_emplacement>: emplacement de l'image sur le partage réseau ; utilisez des guillemets doubles autour du nom de l'emplacement. Voir des exemples de chemin de fichier d'image dans la section Configuration du partage de fichiers à distance à l'aide de l'interface Web

`-s` : affiche l'état actuel

REMARQUE : Tous les caractères, notamment les caractères alphanumériques et spéciaux, peuvent figurer dans le nom d'utilisateur, le mot de passe et l'emplacement de l'image, à l'exception des caractères suivants : ' (guillemet simple), " (guillemets doubles), ,(virgule), < (inférieur à) et > (supérieur à).

Déploiement d'un système d'exploitation à l'aide de Média Virtuel

Avant de déployer un système d'exploitation à l'aide de Média Virtuel, vérifiez que :

- Média Virtuel est *connecté* pour que les lecteurs virtuels apparaissent dans la séquence de démarrage.
- Si Média Virtuel fonctionne en mode de *connexion automatique*, l'application Média Virtuel doit être lancée avant le démarrage du système.
- Le partage de réseau contient les pilotes et un fichier image amorçable du système d'exploitation dans un format standard, tel que **.img** ou **.iso**.

Pour déployer un système d'exploitation à l'aide de Média Virtuel :

1. Effectuez l'une des opérations suivantes :
   - Insérez le CD ou le DCD du système d'installation dans le lecteur de CD ou DVD de la station de gestion.
   - Connectez l'image du système d'exploitation.
2. Sélectionnez le lecteur sur la station de gestion avec l'image nécessaire pour l'associer.
3. Procédez de l'une des manières suivantes pour démarrer depuis le périphérique approprié :
   - Définissez la séquence de démarrage pour démarrer une fois depuis la **disquette virtuelle** ou le **CD/DVD/ISO virtuel** à l'aide de l'interface Web iDRAC7.
   - Définissez la séquence de démarrage via **Configuration du système** → **Paramètres du BIOS du système** en appuyant sur <F2> lors du démarrage.
4. Redémarrez le système géré et suivez les instructions qui s'affichent pour effectuer le déploiement.

Liens connexes

Configuration de Média Virtuel
Définition du premier périphérique de démarrage
Configuration d'iDRAC7

Installation d'un système d'exploitation depuis plusieurs disques

1. Dissociez le CD/DVD existant.
2. Insérez le CD/DVD suivant dans le lecteur optique distant.
3. Associez de nouveau le lecteur de CD/DVD.

Déploiement d'un système d'exploitation intégré sur une carte SD

Pour installer un hyperviseur intégré sur une carte SD :

1. Insérez les deux cartes SD dans les logements IDSDM (Internal Dual SD Module) sur le système.
2. Activez le module et la redondance SD (si nécessaire) dans le BIOS.
3. Vérifiez que la carte SD est disponible sur l'un des lecteurs lorsque vous appuyez sur <F11> lors du démarrage.
4. Déployez le système d'exploitation intégré et suivez les instructions d'installation.

Liens connexes

À propos d'IDSDM
Activation du module SD et de la redondance dans le BIOS

Activation du module SD et de la redondance dans le BIOS

Pour activer le module SD et la redondance dans le BIOS :

1. Appuyez sur <F2> lors du démarrage.
2. Accédez à **Configuration du système** → **Paramètres du BIOS du système** → **Périphériques intégrés**.
3. Affectez à **Port USB interne** la valeur **Actif**. Si la valeur est **Inactif**, IDSDM n'est pas disponible comme périphérique de démarrage.
4. Si la redondance n'est pas nécessaire (carte SD unique), affectez à **Port de carte SD interne** la valeur **Actif** et à **Redondance de carte SD interne** la valeur **Désactivé**.
5. Si la redondance est nécessaire (deux cartes SD), affectez à **Port de carte SD interne** la valeur **Actif** et à **Redondance de carte SD interne** la valeur **Miroir**.
6. Cliquez sur **Retour**, puis sur **Terminer**.
7. Cliquez sur **Oui** pour enregistrer les paramètres et appuyez sur <Échap> pour quitter le programme de **Configuration du système**.

À propos d'IDSDM

Le module IDSDM (Internal Dual SD Module) est disponible uniquement sur les plates-formes applicables. IDSDM fournit une 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.

L'une ou l'autre des cartes SD peut être la carte principale. Par exemple, si deux nouvelles cartes SD sont installées dans le module IDSDM, SD1 est active (carte principale) et SD2 est la carte de secours. Les données sont écrites sur les deux cartes, mais elles sont lues sur SD1. Si la carte SD1 est défaillante ou supprimée, SD2 devient automatiquement la carte active (carte principale).

Vous pouvez afficher l'état, l'intégrité et la disponibilité d'IDSDM en utilisant l'interface Web iDRAC7 ou l'interface RACADM. L'état de redondance et les événements d'erreur de la carte SD sont consignés dans le journal SEL affiché sur le panneau avant, et des alertes PET sont générées si les alertes sont activées.

Liens connexes

Affichage des informations des capteurs

19
Dépannage d'un système géré à l'aide d'iDRAC7

Vous pouvez identifier et résoudre les problèmes d'un système géré en utilisant :

- la console de diagnostic ;
- le code Post ;
- les vidéos de démarrage et de blocage ;
- l'écran du dernier blocage système ;
- les journaux d'événements du système ;
- les journaux Lifecycle ;
- l'état du panneau avant ;
- les voyants des pannes ;
- l'intégrité du système.

Liens connexes

Utilisation de la console de diagnostic
Planification de diagnostics automatisés à distance
Affichage des codes Post
Affichage des vidéos de capture de démarrage et de blocage
Affichage des journaux
Affichage de l'écran du dernier blocage du système
Affichage de l'état du panneau avant
Voyants des problèmes matériels
Affichage de l'intégrité du système
Création d'un rapport de support technique

Utilisation de la console de diagnostic

iDRAC7 fournit un ensemble d'outils standard de diagnostic réseau similaires aux outils des systèmes Microsoft Windows et Linux. En utilisant l'interface Web iDRAC7, vous pouvez accéder aux outils de débogage réseau.

Pour accéder à la console de diagnostic :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Dépannage** → **Diagnostics**.
2. Dans la zone de texte **Commandes**, entrez une commande et cliquez sur **Envoyer**. Pour plus d'informations sur les commandes, voir l'*Aide en ligne d'iDRAC7*.

   Les résultats s'affichent sur la même page.

Planification de diagnostics automatisés à distance

Vous pouvez demander des diagnostics automatisés à distance hors ligne sur un serveur en tant qu'événement ponctuel et renvoyer les résultats. Si les diagnostics nécessitent un redémarrage, vous pouvez redémarrer immédiatement ou les planifier lors d'un cycle de maintenance ou un redémarrage suivant (similaire à des mises à jour). Lorsque les diagnostics sont exécutés, les résultats sont collectés et stockés dans le stockage interne d'iDRAC. Vous pouvez alors

exporter les résultats vers un partage réseau CIFS ou NFS à l'aide de la commande racdam `diagnostics export`. Vous pouvez également exécuter les diagnostics à l'aide des commandes WSMAN appropriées. Pour plus d'informations, voir la documentation de WSMAN.

Vous devez disposer de la licence iDRAC7 Express pour utiliser les diagnostics automatisés à distance.

Vous pouvez exécuter les diagnostics immédiatement ou les planifier à un certain jour et à une certaine heure, spécifier le type de diagnostics, et le type de redémarrage.

Pour la planification, vous pouvez spécifier les éléments suivants :

- Heure de début : pour exécuter le diagnostic à un jour et à une date ultérieurs. Si vous spécifiez TIME NOW, le diagnostic s'exécute au prochain redémarrage.
- Heure de fin : pour exécuter le diagnostic à un jour et une heure postérieurs à l'heure de début. S'il n'est pas lancé avant l'heure de fin, il est marqué comme étant en échec avec Heure de fin expiré. Si vous spécifiez TIME NA, le temps d'attente n'est pas applicable.

Les types de tests de diagnostic sont les suivants :

- Test express
- Test étendu
- Les deux dans une séquence

Les types de redémarrage sont les suivants :

- Cycle d'alimentation du système
- Arrêt normal (attend la mise hors tension du système d'exploitation ou le redémarrage du système)
- Arrêt normal forcé (signale au système d'exploitation de s'éteindre et attend 10 minutes. Si le système d'exploitation ne s'éteint pas, l'iDRAC effectue un cycle d'alimentation du système)

Une seule tâche de diagnostic peut être programmée ou exécutée à un moment donné. Une tâche de diagnostic peut réussir, réussir avec une erreur ou ne pas aboutir. Les événements de diagnostic, notamment les résultats sont enregistrés dans le journal du Lifecycle Controller. Vous pouvez récupérer les résultats de la dernière exécution de diagnostic à l'aide de la RACADM ou de la WSMAN distante.

Vous pouvez exporter les résultats des diagnostics des derniers tests de diagnostic terminés qui ont été programmés à distance sur un partage réseau comme CIFS ou NFS. La taille de fichier maximale est de 5 Mo.

Vous pouvez annuler une tâche de diagnostic lorsque l'état de la tâche est Non planifié ou Planifié. Si le diagnostic est en cours d'exécution, redémarrez le système pour annuler la tâche.

Avant d'exécuter des diagnostics à distance, assurez-vous que :

- Le Lifecycle Controller est activé.
- Vous avez des droits de connexion et de contrôle du serveur.

Planification des diagnostics automatisés à distance à l'aide de RACADM

Pour exécuter les diagnostics à distance et enregistrer les résultats sur le système local, utilisez la commande suivante :

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e
<Expiration Time>
```

Pour exporter les résultats de la dernière exécution de tests de diagnostic à distance, utilisez la commande suivante :

```
racadm diagnostics export -f <file name> -l <NFS / CIFS share> -u <username> -p
<password>
```

Pour plus d'informations sur ces options, voir le manuel *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC*, disponible à l'adresse **dell.com/support/manuals**.

Affichage des codes Post

Les codes Post sont des indicateurs d'avancement du BIOS du système, qui indiquent les étapes de la séquence de démarrage depuis une réinitialisation avec mise sous tension. Ils permettent d'identifier les problèmes liés au démarrage du système. La page **Codes du Post** affiche le dernier code Post système avant le démarrage du système.

Pour afficher les codes Post, accédez à **Présentation générale → Serveur → Dépannage → Code du Post**.

La page **Code du POST** affiche l'indicateur d'intégrité du système, un code hexadécimal et la description du code.

Affichage des vidéos de capture de démarrage et de blocage

Vous pouvez afficher les vidéos de :

- Trois derniers cycles de démarrage : une vidéo de cycle de démarrage enregistre la séquence des événements d'un cycle de démarrage. Les vidéos de cycle de démarrage sont organisées du dernier démarrage au premier démarrage.
- Vidéo du dernier blocage : une vidéo de blocage enregistre la séquence d'événements précédant le blocage.

Il s'agit d'une fonction sous licence.

iDRAC7 enregistre cinquante trames au cours du démarrage. La lecture des écrans de démarrage s'effectue à raison d'une trame par seconde. Si iDRAC7 est réinitialisé, la vidéo de capture de démarrage n'est pas disponible, car elle est stockée en mémoire RAM et supprimée.

REMARQUE : Vous devez disposer des privilèges d'accès à la console virtuelle ou Administrateur pour lire les vidéo de capture de démarrage et de blocage.

Pour afficher l'écran de **capture du démarrage**, cliquez sur **Présentation générale → Serveur → Dépannage → Capture vidéo**.

L'écran **Capture vidéo** affiche les enregistrements vidéo. Pour plus d'informations, voir l'*aide en ligne d'iDRAC7*.

Affichage des journaux

Vous pouvez afficher les journaux SEL (System Event Logs) et les journaux Lifecycle. Pour plus d'informations, voir Affichage du journal des événements système et Affichage du journal Lifecycle .

Affichage de l'écran du dernier blocage du système

La fonction d'écran du dernier blocage crée une capture d'écran du dernier blocage du système, l'enregistre et l'affiche dans iDRAC7. Cette fonction est disponible sous licence.

Pour afficher l'écran du dernier blocage :

1. Vérifiez que la fonction d'écran du dernier blocage système est activée.
2. Dans l'interface Web iDRAC7, accédez à **Présentation générale → Serveur → Dépannage → Dernier écran de blocage**.

   La page **Dernier écran de blocage** affiche le dernier écran de blocage enregistré du système géré.

   Cliquez sur **Effacer** pour supprimer le dernier écran de blocage.

Liens connexes

Activation du dernier écran de blocage

Affichage de l'état du panneau avant

Le panneau avant du système géré résume l'état des composants suivants du système :

- Batteries
- Ventilateurs
- Intrusion
- Blocs d'alimentation
- Média Flash amovible
- Températures
- Tensions

Vous pouvez afficher l'état du panneau avant du système géré :

- Pour les serveurs en rack et de type tour : état du panneau avant LCD et du voyant LED d'ID système ou état du panneau avant LED et voyant d'ID système.
- Pour les serveurs lames : uniquement les voyants d'ID système.

Affichage de l'état du panneau avant LCD

Pour afficher l'état du panneau avant LCD des serveurs en rack et de type tour applicables, dans l'interface Web iDRAC7, accédez à **Présentation générale → Matériel → Panneau avant** . La page **Panneau avant** s'affiche.

La section **Affichage dynamique du panneau avant** contient les messages actuellement affichés sur le panneau avant LCD. Lorsque le système fonctionne normalement (voyant bleu fixe sur le panneau avant LCD), **Masquer l'erreur** et **Afficher l'erreur** sont estompés. Vous pouvez masquer ou afficher les erreurs uniquement pour les serveurs rack et de type tour.

Pour afficher l'état du panneau avant LCD en utilisant l'interface RACADM, utilisez les objets du groupe `System.LCD`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Liens connexes

Configuration du paramétrage LCD

Affichage de l'état LED du panneau avant du système

Pour afficher l'état LED d'ID système en cours, dans l'interface Web iDRAC7, accédez à **Présentation générale → Matériel → Panneau avant**. La section **Données dynamiques du panneau avant** affiche l'état actuel du panneau avant :

- Bleu fixe : aucune erreur sur le système géré.
- Bleu clignotant : le mode d'identification est activé (qu'il existe une erreur ou non sur le système géré).
- Orange fixe : le système géré est en mode Failsafe.
- Orange clignotant : erreur sur le système géré.

Lorsque le système fonctionne normalement (indiqué par une icône d'intégrité bleue sur le panneau avant LED), **Masquer l'erreur** et **Afficher l'erreur** sont estompés. Vous pouvez afficher ou masquer les erreurs uniquement pour les serveurs en rack et de type tour.

Pour afficher l'état du LED d'ID système en utilisant l'interface RACADM, utilisez la commande **getled**. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Liens connexes

Configuration du paramétrage LED d'ID système

Voyants des problèmes matériels

Les problèmes matériels sont les suivants :

- Défaillance de la mise sous tension
- Ventilateurs bruyants
- Perte de connectivité réseau
- Défaillance du disque dur
- Défaillance du média USB
- Endommagement physique

En fonction du problème, utilisez les méthodes suivantes pour éliminer le problème :

- Remettez le module ou le composant en place et redémarrez le système.
- S'il s'agit d'un serveur lame, insérez le module dans une autre baie dans le châssis.
- Remplacez les disques durs ou les lecteurs Flash USB
- Reconnectez ou remplacez les câbles d'alimentation et les câbles réseau

Si le problème persiste, voir le *Manuel du propriétaire du matériel* pour les informations de dépannage sur le périphérique matériel.

PRÉCAUTION : Vous devez exécuter les opérations de dépannage et de réparation simples indiquées dans la documentation du produit ou conformément aux instructions du service de maintenance téléphonique et du support technique. Les endommagements résultant d'opérations de maintenance non autorisées par Dell ne sont pas couverts par la garantie. Lisez et suivez les instructions de sécurité fournies avec le produit.

Affichage de l'intégrité du système

Les interfaces iDRAC7 et CMC (pour les serveurs lames) affichent l'état des éléments suivants :

- Batteries
- Ventilateurs
- Intrusion
- Blocs d'alimentation
- Média Flash amovible
- Températures
- Tensions
- UC

Dans l'interface Web iDRAC7, accédez à **Présentation générale → Serveur → Résumé du système → Intégrité du système**.

Pour afficher l'intégrité de l'UC, accédez à **Présentation générale → Matériel → UC**.

Les voyants d'intégrité du système sont les suivants :

- — Indique un état normal.
- — Indique un état d'avertissement.

-  — Indique un état de défaillance.
-  — Indique un état inconnu

Cliquez sur un nom de composant dans la section **Intégrité du serveur** pour afficher des informations sur le composant.

Création d'un rapport de support technique

Si vous devez travailler avec le support technique sur un problème avec un serveur, mais que la politique de sécurité locale empêche la connexion Internet directe, vous pouvez fournir au support technique les données nécessaires pour faciliter le dépannage du problème sans avoir à installer de logiciel ou à télécharger des outils de Dell et sans avoir accès à Internet depuis le système d'exploitation du serveur ou iDRAC. Vous pouvez envoyer le rapport à partir d'un autre système et être certain que les données collectées à partir de votre serveur ne sont pas visibles par des individus non autorisés lors de la transmission au support technique.

Vous pouvez générer un rapport d'intégrité du serveur, puis l'exporter dans un emplacement situé sur la station de gestion (local) ou dans un emplacement réseau partagé, tel que les protocoles CIFS (Common Internet File System) ou un partage de fichiers en réseau (NFS). Vous pouvez ensuite partager ce rapport directement avec le support technique. Pour exporter vers un partage réseau tel que CIFS ou NFS, la connectivité réseau directe au port réseau iDRAC partagé ou dédié est requise.

Le rapport est généré au format ZIP standard. Le rapport contient des informations similaires aux informations disponibles dans le rapport DSET, mais uniquement les informations sur le matériel et la plus récente des entrées de journal Lifecycle Controller (les entrées archivées ne sont pas incluses).

Une fois le rapport généré, vous pouvez supprimer les informations que vous ne souhaitez pas partager avec le support technique.

Chaque fois que la collecte de données est effectuée, un événement est enregistré dans le journal du Lifecycle Controller. L'événement inclut des informations telles que l'interface utilisée, la date et l'heure de l'exportation et le nom d'utilisateur iDRAC.

Création d'un rapport de support technique à l'aide de l'interface Web

Avant de générer le rapport, assurez-vous que :

- Lifecycle Controller et CSIOR (Collect System Inventory On Reboot) sont activés.
- Vous avez des droits de connexion et de contrôle du serveur.

Pour générer le rapport contenant les informations de support, procédez comme suit :

1. Dans l'interface Web iDRAC, allez à **Présentation générale** → **Serveur** → **Dépannage** → **Rapport de support technique** .

   La page **Rapport de support technique** s'affiche.
2. Sélectionnez une des options suivantes :

   – **Local** : exportez le rapport vers un emplacement situé sur le système local.

   – **Réseau** : exportez le rapport vers un partage réseau et spécifiez les paramètres réseau.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne iDRAC7*.

3. Cliquez sur **Exporter**.

   Les informations sont collectées et exportées vers l'emplacement spécifié au format **.zip**.

   Si vous exportez le rapport sans privilèges de **connexion** et de **contrôle du serveur**, un message d'erreur s'affiche.

   Si le Lifecycle Controller est désactivé ou en état de récupération, un message d'avertissement et les étapes d'activation de Lifecycle Controller s'affichent.

   Si la fonction CSIOR est désactivée, un message s'affiche indiquant que les données en cours d'exportation peuvent ne pas être les données les plus récentes.

Vérification des messages d'erreur dans l'écran d'état du serveur

Lorsqu'un voyant orange clignote et qu'un serveur est défaillant, l'écran principal d'état du serveur sur l'écran LCD indique en orange le serveur affecté. Utilisez les boutons de navigation de l'écran LCD pour sélectionner le serveur concerné, puis cliquez sur le bouton du milieu. Les messages d'erreur et d'avertissement s'affichent sur la deuxième ligne. Pour la liste des messages d'erreur affichés sur l'écran LCD, voir le manuel du propriétaire du serveur.

Redémarrage d'iDRAC7

Vous pouvez redémarrer iDRAC7 à chaud ou à froid sans mettre le serveur hors tension :

- Redémarrage à froid : sur le serveur, appuyez sur le bouton LED et maintenez-le enfoncé pendant 15 secondes.
- Redémarrage à chaud : utilisez l'interface Web iDRAC7 ou l'interface RACADM.

Réinitialisation d'iDRAC7 en utilisant l'interface Web iDRAC7

Pour redémarrer iDRAC7, procédez de l'une des manières suivantes dans l'interface Web iDRAC7 :

- Accédez à **Présentation générale** → **Serveur** → **Résumé**. Sous **Tâches de lanceme.nt rapide**, cliquez sur **Réinitialiser iDRAC**.
- Accédez à **Présentation générale** → **Serveur** → **Dépannage** → **Diagnostics**. Cliquez sur **Réinitialiser iDRAC**.

Réinitialisation d'iDRAC7 en utilisant l'interface RACADM

Pour redémarrer iDRAC7, utilisez la commande **racreset**. Pour plus d'informations, voir le *RACADM Reference Guide for iDRAC7 and CMC* (Guide de référence RACADM d'iDRAC7 et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Restauration des paramètres par défaut définis en usine d'iDRAC7

Vous pouvez restaurer les paramètres par défaut définis en usine d'iDRAC7 à l'aide de l'utilitaire Paramètres iDRAC ou de l'interface Web iDRAC7.

Restauration des paramètres par défaut définis en usine d'iDRAC7 à l'aide de l'interface Web iDRAC7

Pour restaurer les paramètres par défaut définis en usine d'iDRAC7 à l'aide de l'interface Web iDRAC7 :

1. Allez à **Présentation** → **Serveur** → **Dépannage** → **Diagnostics**.
   La page **Diagnostics de la console** s'affiche.
2. Cliquez sur **Réinitialiser iDRAC sur les paramètres par défaut**.
   L'état d'avancement s'affiche en pourcentage. L'iDRAC7 redémarre et est restaurée sur ses paramètres par défaut. L'IP d'iDRAC7 est réinitialisée et n'est pas accessible. Vous pouvez configurer l'IP à l'aide du panneau avant ou du BIOS.

Restauration des paramètres par défaut définis en usine d'iDRAC à l'aide de l'utilitaire Paramètres iDRAC7

Pour restaurer les paramètres par défaut définis en usine d'iDRAC7 en utilisant l'utilitaire de configuration d'iDRAC :

1. Allez à **Restauration des configurations par défaut iDRAC**.
   La page **Paramètres iDRAC - Restauration des configurations par défaut iDRAC** s'affiche.
2. Cliquez sur **Oui**.
   La réinitialisation iDRAC démarre.
3. Cliquez sur **Retour** et accédez à la même page **Restauration des configurations par défaut iDRAC** pour afficher le message d'aboutissement.

20

Questions fréquemment posées

Cette section contient les questions courantes sur les éléments suivants :

Journal des événements système

Lors de l'utilisation de l'interface Web iDRAC7 via Internet Explorer, pourquoi le journal SEL ne peut-il pas être enregistré avec l'option Enregistrer sous ?

Ce problème provient d'un paramètre du navigateur. Pour le résoudre :

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 iDRAC7 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 :
   - Demander confirmation pour les téléchargements de fichiers (si cette option est disponible)
   - Téléchargement de fichiers

   PRÉCAUTION : Pour être certain que l'ordinateur utilisé pour accéder à iDRAC7 est fiable, sous Divers, désélectionnez l'option Démarrage des applications et des fichiers non sûrs.

Sécurité du réseau

Lors de l'accès à l'interface Web d'iDRAC7, un avertissement de sécurité s'affiche pour indiquer que le certificat SSL émis par l'autorité de certification (CA) n'est pas autorisé.

iDRAC7 contient un certificat de serveur par défaut iDRAC7 pour protéger le réseau lors de l'accès via l'interface Web et l'interface distante RACADM. Ce certificat n'est pas émis par une autorité CA de confiance. Pour résoudre ce problème, téléversez un certificat de serveur iDRAC7 émis par une CA de confiance (par exemple, Microsoft Certificate Authority, Thawte ou Verisign).

Pourquoi le serveur DNS n'enregistre pas iDRAC7 ?

Certains serveurs DNS enregistrent les noms iDRAC7 qui contiennent jusqu'à 31 caractères.

Lors de l'accès à l'interface Web d'iDRAC7, un avertissement de sécurité s'affiche pour indiquer que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte iDRAC7.

iDRAC7 inclut un certificat de serveur iDRAC7 par défaut pour protéger le réseau lors de l'accès à l'interface Web et à l'interface distante RACADM. Lorsque ce certificat est utilisé, le navigateur Web affiche un avertissement de sécurité, car le certificat par défaut émis pour iDRAC7 ne correspond pas au nom d'hôte iDRAC7 (par exemple, l'adresse IP).

Pour résoudre ce problème, téléversez un certificat de serveur iDRAC7 émis vers l'adresse ou le nom d'hôte iDRAC7. Lors de la génération du fichier RSC (utilisé pour l'émission du certificat), veillez à ce que le nom commun (CN) du fichier RSC corresponde à l'adresse IP iDRAC7 (si le certificat est émis vers IP) ou au nom iDRAC7 DNS enregistré (si le certificat est émis vers le nom enregistré iDRAC7).

Pour que le fichier RSC corresponde au nom iDRAC7 DNS enregistré :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Paramètres iDRAC** → **Réseau** . La page **Réseau** s'affiche.
2. Dans la section **Paramètres communs** :
   - Sélectionnez l'option **Enregistrer iDRAC sur DNS**.
   - Dans le champ **Nom IDRAC DNS**, saisissez le nom iDRAC7.
3. Cliquez sur **Appliquer**.

Active Directory

L'ouverture de session dans Active Directory a échoué. Comment résoudre ce problème ?

Pour identifier la cause du problème, dans la page **Configuration et gestion d'Active Directory**, cliquez sur **Tester les paramètres**. Vérifiez les résultats du test et résolvez le problème. Changez la configuration et exécutez le test jusqu'à ce que l'utilisateur de test passe l'étape d'autorisation.

En général, vérifiez les éléments suivants :

- Tout en étant connecté, veillez à utiliser le nom de domaine d'utilisateur correct et non pas le nom NetBIOS. Si vous disposez d'un compte d'utilisateur iDRAC7 local, ouvrez une session dans iDRAC7 à l'aide des données d'identification locales. Après la connexion, vérifiez que :
  - L'option **Activation Active Directory** est sélectionnée dans la page **Configuration et gestion d'Active Directory**.
  - Le paramètre DNS est correct dans la page **Configuration réseau iDRAC7** .
  - Le certificat CA racine Active Directory correct est téléversé vers iDRAC7 si la validation de certificat a été activée.
  - Le nom iDRAC et le nom de domaine iDRAC correspondent à la configuration de l'environnement Active Directory si vous utilisez le schéma étendu.
  - Le nom de groupe et le nom de domaine correspondent à la configuration Active Directory si vous utilisez le schéma standard.
- Vérifiez les certificats SSL des contrôleurs de domaine pour vous assurer que l'heure iDRAC7 est comprise dans la période de validité du certificat.

L'ouverture de session Active Directory échoue si la validation de certificat est activée. Les résultats du test contiennent le message d'erreur suivant. Pourquoi et comment résoudre le problème ?

```
ERREUR : impossible de contacter le serveur LDAP, erreur :14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE: échec de la vérification du certificat :
vérifiez que le certificat d'autorité de certification (CA) correct a été
téléversé vers iDRAC7. Vérifiez également que la date iDRAC7 se trouve dans la
période de validité des certificats et que l'adresse du contrôleur de domaine
définie dans iDRAC7 correspond à l'objet du certificat du service d'annuaire.
```

Si la validation de certificat est activée, lorsque iDRAC7 établit la connexion SSL avec le serveur d'annuaire, il utilise le certificat CA téléversé pour vérifier le certificat du serveur d'annuaire. Les principales causes de l'échec de la validation de certification sont les suivantes :

- La date iDRAC7 ne se trouve pas dans la période de validité du certificat du serveur ou du certificat CA. Vérifiez l'heure iDRAC7 et la période de validité de votre certificat.
- Les adresses des contrôleurs de domaine définies dans iDRAC7 ne correspondent pas à l'objet ou à l'autre nom d'objet du certificat du serveur d'annuaire. Si vous utilisez une adresse IP, lisez la question suivante. Si vous utilisez le nom de domaine complet qualifié, veillez à utiliser le nom de domaine complet qualifié du contrôleur de domaine et non pas le domaine. Par exemple, **nomserveur.exemple.com** au lieu de **exemple.com**.

La validation de certificat échoue si l'adresse IP est utilisée comme adresse de contrôleur de domaine. Comment résoudre ce problème ?

Vérifiez le champ Objet ou Autre nom d'objet du certificat du contrôleur de domaine. Normalement, Active Directory utilise le nom d'hôte et non pas l'adresse IP du contrôleur de domaine dans le champ Objet ou Autre nom de l'objet du certificat du contrôleur de domaine. Pour résoudre ce problème, procédez de l'une des manières suivantes :

- Définissez le nom d'hôte (nom de domaine complet qualifié) du contrôleur de domaine comme *adresse(s) de contrôleur de domaine* dans iDRAC7 pour qu'il corresponde au champ Objet ou Autre nom de l'objet dans le certificat du serveur.
- Réémettez le certificat de serveur pour utiliser une adresse IP dans le champ Objet ou Autre nom de l'objet pour qu'il corresponde à l'adresse IP définie dans iDRAC78.
- Désactivez la validation de certificat si vous choisissez de faire confiance à ce contrôleur de domaine sans validation de certificat los de l'établissement de liaisons SSL.

Comment configurer l'adresse (ou les adresses) de contrôleur de domaine en utilisant le schéma étendu dans un environnement multi-domaine ?

Il doit s'agir du nom d'hôte (nom de domaine complet qualifié) ou de l'adresse IP du (ou des contrôleurs) de domaine qui gère le domaine dans lequel l'objet iDRAC7 réside.

Quand faut-il définir une adresse (ou des adresses) de catalogue global ?

Si vous utilisez le schéma standard et que les utilisateurs et les groupes de rôles appartiennent à des domaines différents, une adresse (ou plusieurs adresses) de catalogue global est nécessaire. Dans ce cas, vous pouvez utiliser uniquement le groupe universel.

Si vous utilisez le schéma standard et que tous les utilisateurs et groupes de rôles proviennent du même domaine, une ou des adresses du catalogue global ne sont pas requises.

Si vous utilisez le schéma étendu, l'adresse du catalogue global n'est pas utilisée.

Comment fonctionne la requête de schéma standard ?

iDRAC7 se connecte tout d'abord à l'adresse (ou aux adresses) de contrôleur de domaine définie. Si l'utilisateur et les groupes de rôles se trouvent dans ce domaine, les privilèges seront enregistrés.

Si une adresse (ou des adresses) de contrôleur global est configurée, iDRAC7 continue d'interroger le catalogue global. Si des privilèges supplémentaires sont extraits du catalogue global, ces privilèges sont accumulés.

iDRAC7 utilise-t-il toujours LDAP sur SSL ?

Oui. Tout le transport s'effectue sur le port 636 et/ou 3 269. Au cours du test, iDRAC7 exécute LDAP CONNECT uniquement pour isoler le problème, mais il n'exécute pas LDAP BIND sur une connexion non sécurisée.

Pourquoi iDRAC7 active-t-il par défaut la validation de certificat ?

iDRAC7 applique une sécurité stricte pour garantir l'identité du contrôleur de domaine auquel iDRAC7 se connecte. Sans la validation de certificat un intrus peut usurper l'identité d'un contrôleur de domaine et détourner la connexion SSL. Si vous faites confiance à tous les contrôleurs de domaine dans votre limite de sécurité sans la validation de certificat, vous pouvez la désactiver via l'interface Web ou l'interface RACADM.

iDRAC7 prend-il en charge le nom NetBIOS ?

Pas dans cette version.

Pourquoi l'ouverture de session dans iDRAC7 par carte à puce ou connexion directe Active Directory prend-elle jusqu'à quatre minutes ?

L'ouverture de session par carte à puce ou connexion directe Active Directory dure moins de 10 secondes normalement, mais elle peut prendre jusqu'à quatre minutes si vous avez défini le serveur DNS préféré et le serveur DNS secondaire et qu'une erreur s'est produite au niveau du serveur DNS préféré. Des expirations DNS se produisent lorsqu'un serveur DNS est arrêté. iDRAC7 vous connecte à l'aide du serveur DNS secondaire.

Active Directory est configuré pour un domaine présent dans Active Directory Windows Server 2008. 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 membre du groupe. Lors de l'ouverture d'une session dans iDRAC7 en utilisant l'utilisateur présent dans le domaine enfant, l'ouverture de session par connexion directe Active Directory échoue.

Ce problème peut être provoqué par un type de groupe incorrect. Il existe deux types de groupes dans le serveur Active Directory :

- Sécurité : les groupes de sécurité permettent de gérer l'accès des utilisateurs et des ordinateurs aux ressources partagées et de filtrer les paramètres de stratégies de groupe.
- Distribution : les groupes de distribution servent exclusivement de listes de distribution par e-mail.

Veillez à toujours utiliser le type de groupe Sécurité. Vous ne pouvez pas utiliser des groupes de distribution pour affecter des droits à un objet. Utilisez-les pour filtrer les paramètres de stratégie de groupe.

Connexion directe

L'ouverture de session par connexion directe échoue sur Windows Server 2008 R2 x64. Quels sont les paramètres à définir pour résoudre le problème ?

1. Exécutez **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** pour le contrôleur de domaine et la stratégie de contrôleur et de domaine.
2. Configurez les ordinateurs pour qu'ils utilisent la suite de chiffrement DES-CBC-MD5.

   Ces paramètres peuvent affecter la compatibilité avec les ordinateurs clients ou les services et les applications de votre environnement. L'option de configuration des types de chiffrement autorisés pour le paramétrage de stratégie Kerberos se trouve dans **Configuration de l'ordinateur** → **Paramètres de sécurité** → **Stratégies locales** → **Options de sécurité**.
3. Vérifiez que les clients du domaine disposent de l'objet de stratégie de groupe à jour.
4. Sur la ligne de commande, tapez `gpupdate /force` et supprimez l'ancien fichier keytab avec la commande `klist purge`.
5. Après avoir mis à jour l'objet de stratégie de groupe, créez le nouveau fichier keytab.
6. Téléversez le fichier keytab vers iDRAC7.

Vous pouvez désormais ouvrir une session dans iDRAC via la connexion directe.

Pourquoi l'ouverture de session par connexion directe échoue-t-elle avec les utilisateurs Active Directory sur Windows 7 et Windows Server 2008 R2 ?

Vous devez activer les types de cryptage pour Windows 7 et Windows Server 2008 R2. Pour activer les types de cryptage :

1. Ouvrez une session comme administrateur ou utilisateur doté du privilège d'administration.
2. Accédez à **Démarrer** et exécutez **gpedit.msc**. La fenêtre de **Éditeur de stratégie de groupe** s'affiche.

3. Accédez à **Paramètres de l'ordinateur local → Paramètres Windows → Paramètres de sécurité → Stratégies locales → Options de sécurité.** .
4. Cliquez avec le bouton droit de la souris sur **Sécurité réseau : Configurer les types de cryptage autorisés pour Kerberos** et sélectionnez **Propriétés**.
5. Activez toutes les options.
6. Cliquez sur **OK**. Vous pouvez désormais ouvrir une session dans iDRAC via la connexion directe.

Définissez les paramètres supplémentaires suivants pour le schéma étendu :

1. Dans la fenêtre de **Éditeur de stratégie de groupe locale**, accédez à **Paramètres de l'ordinateur local → Paramètres Windows → Paramètres de sécurité → Stratégies locales → Options de sécurité** .
2. Cliquez avec le bouton droit de la souris sur **Sécurité réseau : Restreindre NTLM : trafic NTLM sortant vers le serveur distant** et sélectionnez **Propriétés**.
3. Cliquez sur **Autoriser tous**, puis sur **OK** et fermez la fenêtre **Éditeur de stratégie de groupe local**.
4. Accédez à **Démarrer** et exécutez cmd. La fenêtre de l'invite de commande s'affiche.
5. Exécutez la commande `gpupdate /force`. Les stratégies de groupe sont mises à jour. Fermez la fenêtre de l'invite de commande.
6. Accédez à **Démarrer** et exécutez regedit. La fenêtre **Éditeur de registre** s'affiche.
7. Accédez à **HKEY_LOCAL_MACHINE → System → CurrentControlSet → Control → LSA**.
8. Dans le volet de droite, cliquez avec le bouton droit de la souris et sélectionnez .**Nouvelle → Valeur DWORD (32 bits)** .
9. Nommez la nouvelle clé **SuppressExtendedProtection**.
10. Cliquez avec le bouton droit de la souris sur **SuppressExtendedProtection** et cliquez sur **Modifier.**
11. Dans le champ de données **Valeur**, tapez **1** et cliquez sur **OK**.
12. Fermez la fenêtre de l'**éditeur de registre**. Maintenant, vous pouvez ouvrir une session dans iDRAC7 en utilisant la connexion directe.

Si vous avez activé la connexion directe pour iDRAC et utilisez Internet Explorer pour ouvrir une session dans iDRAC, la connexion directe échoue et le système demande d'entrer vos nom d'utilisateur et mot de passe.

Vérifiez que l'adresse IP d'iDRAC7 figure dans **Outils → Options Internet → Sécurité → Sites de confiance**. Si tel n'est pas le cas, la connexion directe échoue et un message vous invite à entrer votre nom d'utilisateur et votre mot de passe. Cliquez sur **Annuler** et continuez.

Ouverture de session par carte à puce

L'ouverture de session dans iDRAC7 peut prendre jusqu'à quatre minutes à l'aide d'une carte à puce Active Directory.

L'ouverture de session normale par carte à puce Active Directory prend moins de 10 secondes. Cependant, elle peut prendre jusqu'à quatre minutes si vous avez défini le serveur DNS préféré et le serveur DNS secondaire dans la page **Réseau** et que le serveur DNS a échoué. Des expirations DNS se produisent lorsqu'un serveur DNS est arrêté. iDRAC7 vous connecte en utilisant le serveur DNS secondaire.

Le plug-in ActiveX ne parvient pas à détecter le lecteur de carte à puce

Vérifiez que la carte à puce est compatible avec le système d'exploitation Microsoft Windows. Windows prend en charge un nombre limité de fournisseurs de services cryptographiques (CSP).

En règle générale, vérifiez si les CSP de cartes à puce sont présents sur un client, 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 la carte à puce et affiche la boîte de dialogue du code PIN.

Le code PIN de la carte à puce est incorrect.

Déterminez si la carte à puce est verrouillée suite à un trop grand nombre de tentatives avec un code PIN incorrect. Dans ce cas, contactez l'émetteur de la carte à puce de l'entreprise pour obtenir une nouvelle carte.

Console virtuelle

Une session de console virtuelle est active, même si vous avez fermé la session dans l'interface Web iDRAC7. Est-ce normal ?

Oui. Fermez la fenêtre du visualiseur de console virtuelle pour quitter la session correspondante.

Est-il possible de démarrer une nouvelle session vidéo de console distante lorsque la vidéo sur le serveur local est désactivée ?

Oui

Pourquoi la vidéo sur le serveur local prend-elle 15 secondes pour s'arrêter après la demande d'arrêt ?

Ceci permet à l'utilisateur local d'agir avant l'arrêt de la vidéo

Existe-t-il un délai lors de l'activation de la vidéo locale ?

Non, la vidéo démarre immédiatement après réception par iDRAC7 de la demande de démarrage de la vidéo locale.

L'utilisateur peut-il également démarrer ou arrêter la vidéo ?

Lorsque la console locale est désactivée, l'utilisateur local ne peut pas démarrer la vidéo.

L'arrêt de la vidéo locale désactive-t-elle aussi le clavier et la souris locaux ?

Non

L'arrêt de la console locale désactive-t-il la vidéo dans la session de console distante ?

Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de console distante.

Quels sont les privilèges nécessaires à un utilisateur iDRAC7 pour démarrer ou arrêter la vidéo sur le serveur local ?

N'importe quel utilisateur doté des privilèges de configuration iDRAC7 peut activer ou désactiver la console locale.

Comment obtenir l'état actuel de la vidéo sur le serveur local ?

L'état est affiché dans la page de la console virtuelle.

Utilisez la commande RACADM `racadm getconfig -g cfgRacTuning` pour afficher l'état dans l'objet `cfgRacTuneLocalServerVideo`.

Ou bien utilisez la commande RACADM suivante depuis une session Telnet, SSH ou distante :

```
racadm -r (iDRAC IP) -u -p getconfig -g cfgRacTuning
```

L'état figure également dans l'écran OSCAR de la console virtuelle. Lorsque la console locale est activée, un état vert apparaît à côté du nom du serveur. Lorsqu'elle est désactivée, un point jaune indique qu'iDRAC7 a verrouillé la console locale.

Pourquoi le bas de l'écran de la fenêtre de la console virtuelle ne s'affiche-t-il pas ?

Vérifiez que la résolution du moniteur de la station de gestion est 1 280 x 1 024.

Pourquoi la fenêtre du visualiseur de la console virtuelle est-elle illisible sur Linux ?

Le visualiseur de console sur Linux nécessite d'utiliser un jeu de caractères UTF-8. Vérifiez vos paramètres régionaux et réinitialisez le jeu de caractères, si nécessaire.

Pourquoi la souris n'est-elle pas synchronisée dans la console texte Linux dans Lifecycle Controller ?

La console virtuelle nécessite le pilote de souris USB, mais ce dernier est disponible uniquement avec le système d'exploitation X-Window. Dans le visualiseur de console virtuelle, procédez comme suit :

- Accédez à l'onglet **Outils** → **Options de session** → **Souris**. Sous **Accélération de la souris**, sélectionnez **Linux**.
- Sous le menu **Outils**, sélectionnez l'option **Pointeur unique**.

Comment synchroniser les pointeurs de souris dans la fenêtre du visualiseur de console virtuelle ?

Avant de démarrer une session de console virtuelle, veillez à sélectionner la souris correspondant à votre système d'exploitation.

Vérifiez que l'option **Pointeur unique** sous **Outils** dans le menu Console virtuelle iDRAC7 est sélectionnée dans le client Console virtuelle iDRAC7. Le mode par défaut est Deux pointeurs.

Est-il possible d'utiliser le clavier et la souris pour installer à distance un système d'exploitation via la console virtuelle ?

Non. Lorsque vous installez un système d'exploitation Microsoft compatible sur un système avec la console virtuelle activée dans le BIOS, un message de connexion EMS est envoyé pour indiquer que vous devez sélectionner **OK** à distance. Vous devez sélectionner **OK** sur le système local ou redémarrer le serveur géré localement, réinstaller, puis arrêter la console virtuelle dans le BIOS.

Ce message est généré par Microsoft pour indiquer que la console virtuelle est activée. Pour que ce message n'apparaisse pas, désactivez toujours la console virtuelle dans l'utilitaire de configuration d'iDRAC avant d'installer à distance un système d'exploitation.

Pourquoi l'indicateur Verr Num n'indique pas l'état Verr Num sur le serveur distant sur la station de gestion ?

Lorsque vous accédez via iDRAC7, l'indicateur Verr Num sur la station de gestion ne correspond pas nécessairement à l'état Verr Num sur le serveur distant. L'état Verr Num dépend du paramétrage sur le serveur distant lors de la connexion de la session distante, quel que soit l'état Verr Num sur la station de gestion.

Pourquoi plusieurs fenêtres de visualiseur de session apparaissent-elles lorsque j'établis une session de console virtuelle à partir de l'hôte local ?

Vous configurez une session de console virtuelle depuis le système local et cette opération n'est pas prise en charge.

Si une session de console virtuelle est en cours et qu'un utilisateur local accède au serveur géré, le premier utilisateur reçoit-il un message d'avertissement ?

Non. Si un utilisateur local accède au système, vous contrôlez tous les deux le système.

Quelle est la bande passante nécessaire pour exécuter une session de console virtuelle ?

Il est recommandé de disposer d'une connexion de 5 MBPS pour obtenir de bonnes performances. Une connexion de 1 MBPS minimum est nécessaire pour obtenir des performances minimales.

Quelle est la configuration système minimale requise pour que la 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.

Pourquoi la fenêtre du visualiseur de console virtuelle affiche-t-elle parfois le message Aucun signal ?

Ce message peut s'afficher si le plug-in de console virtuelle iDRAC7 ne reçoit pas la vidéo du serveur distant. Généralement, cette situation se produit lorsque le serveur distant est arrêté. Il peut arriver que le message s'affiche suite à une mauvaise réception de la vidéo du serveur distant.

Pourquoi la fenêtre du visualiseur de console virtuelle affiche-t-elle parfois le message Hors plage ?

Ce message apparaît, car la valeur d'un paramètre nécessaire pour capturer la vidéo est hors plage et ne permet pas à iDRAC7 de capturer la vidéo. Les paramètres, tels que la résolution d'écran et la vitesse de rafraîchissement, dont la valeur est trop élevée, génèrent ce message. Normalement, les limitations physiques, telles que la taille de mémoire vidéo et la bande passante, définissent la plage de valeurs maximales.

Lors du démarrage d'une session de console virtuelle à partir de l'interface Web iDRAC7, un message contextuel de sécurité ActiveX apparaît. Pourquoi ?

iDRAC7 peut ne pas figurer dans la liste des sites de confiance. Pour que ce message n'apparaisse pas chaque fois que vous lancez une session de console virtuelle, ajoutez iDRAC7 à la liste des sites de confiance dans la navigateur client :

1. Cliquez **Outils** → **Options Internet** → **Sécurité** → **Sites de confiance**.
2. Cliquez sur **Sites** et entrez l'adresse IP ou le nom DNS d'iDRAC7.
3. Cliquez sur **Ajouter**.
4. Cliquez sur **Niveau personnalisé**.
5. Dans la fenêtre **Paramètres de sécurité**, sélectionnez **Demander** sous **Télécharger les contrôles ActiveX non signés**.

Pourquoi la fenêtre du visualiseur de console virtuelle est-elle vide ?

Si vous disposez du privilège Média Virtuel, mais pas du privilège Console virtuelle, vous pouvez démarrer le visualiseur pour accéder à la fonction Média Virtuel, mais la console du serveur géré ne s'affiche pas.

La souris ne se synchronise pas sous DOS pendant l'utilisation de la console virtuelle. Pourquoi ?

Le BIOS Dell émule le pilote de la souris comme souris PS/2. Par nature, la souris PS/2 utilise une position relative pour le pointeur, ce qui génère des délais de synchronisation. iDRAC7 utilise un pilote de souris USB qui utilise le positionnement absolu et une trace de pointeur de souris plus précise. Même si iDRAC7 envoie la position absolue de souris USB au BIOS Dell, l'émulation BIOS convertit la position en position relative et le comportement persiste. Pour résoudre le problème, définissez le mode de souris USC/Diags dans l'écran de configuration.

Après le démarrage de la console virtuelle, le pointeur de la souris est actif dans la console virtuelle, mais pas sur le système local. Quelle est la cause de cette situation et comment résoudre le problème ?

Ce problème apparaît si le **Mode Souris** est **USC/Diags**. Appuyez sur la touche de raccourci **Alt + M** pour utiliser la souris sur le système local. Appuyez de nouveau sur **Alt + M** pour utiliser la souris dans la console virtuelle.

Lorsque l'interface Web iDRAC7 est démarrée depuis l'interface Web CMC, pourquoi la session d'interface graphique expire-t-elle peu après le démarrage de la console virtuelle ?

Lorsque vous démarrez la console virtuelle dans iDRAC7 depuis l'interface Web CMC, une fenêtre contextuelle s'ouvre pour lancer la console virtuelle. Cette fenêtre se ferme peu après l'ouverture de la console virtuelle.

Lors du démarrage de l'interface graphique et de la console virtuelle sur un même système iDRAC7 depuis une station de gestion, une expiration de session se produit pour l'interface graphique iDRAC7 si l'interface graphique est démarrée avant la fermeture de la fenêtre contextuelle. Si vous démarrez l'interface graphique d'iDRAC7 depuis l'interface Web CMC après la fermeture de la fenêtre virtuelle, le problème disparaît.

Pourquoi la touche Linux SysRq ne fonctionne-t-elle pas avec Internet Explorer ?

Le fonctionnement de la touche Linux SysRq change lorsque vous utilisez la console virtuelle depuis Internet Explorer. Pour envoyer la touche SysRq, appuyez sur la touche **Impr écran** et relâchez-la tout en maintenant les touches **Ctrl** et **Alt** enfoncées. Pour envoyer la touche SysRq à un serveur Linux distant via iDRAC7 en utilisant Internet Explorer :

1. Activez la touche de fonction magique sur le serveur Linux distant. Vous pouvez utiliser la commande suivante pour l'activer sur le terminal Linux :
   ```
   echo 1 > /proc/sys/kernel/sysrq
   ```
2. Activez le mode transfert de données clavier du visualiseur Active X.
3. Appuyez sur les touches **Ctrl + Alt + Impr écran**.
4. Relâchez seulement la touche **Impr écran**.
5. Appuyez sur **Impr écran+Ctrl+Alt**.

REMARQUE : La fonction SysRq n'est pas prise en charge actuellement par Internet Explorer et Java.

Pourquoi le message « Liaison interrompue » s'affiche-t-il dans le bas de la console virtuelle ?

Lorsque vous utilisez le port réseau partagé au cours d'un redémarrage du serveur, iDRAC est déconnecté alors que le BIOS réinitialise la carte réseau. Ce délai est plus long sur les cartes 10 Gb et il est également exceptionnellement long

si le protocole STP (Spanning Tree Protocol) est activé sur le commutateur. Dans ce cas, il est recommandé d'activer « portfast » pour le commutateur de port connecté au serveur. Dans la plupart des cas, la console virtuelle se restaure.

Média virtuel

Pourquoi la connexion du client Média Virtuel s'interrompt-elle parfois ?

Si le délai d'attente du réseau expire, le micrologiciel d'iDRAC7 interrompt la connexion en déconnectant la liaison entre le serveur et le lecteur virtuel.

Si vous changez le CD dans le système client, le nouveau CD peut ne pas disposer de la fonction de démarrage automatique. Dans ce cas, le micrologiciel peut expirer et la connexion est perdue si le client prend trop de temps pour lire le CD. Si la connexion est perdue, reconnectez-vous depuis l'interface graphique et poursuivez l'opération .

Si les paramètres de configuration Média Virtuel sont modifiés dans l'interface Web iDRAC7 ou via des commandes RACADM locales, le média connecté est déconnecté lorsque les modifications de configuration sont appliquées.

Pour vous reconnecter au lecteur virtuel, utilisez la fenêtre **Vue client** .

Pourquoi l'installation d'un système d'exploitation Windows via Média Virtuel prend-elle autant de temps ?

Si vous installez le système d'exploitation Windows en utilisant le *DVD Dell Systems Management Tools and Documentation* et que la connexion réseau est lente, la procédure d'installation peut accéder à l'interface Web d'iDRAC7 au bout d'un certain temps du fait de la latence du réseau. La fenêtre d'installation n'indique pas l'avancement de l'installation.

Comment configurer le périphérique virtuel comme périphérique amorçable ?

Sur le système géré, accédez au programme de configuration du BIOS et au menu Boot. Recherchez le CD virtuel, le lecteur de disquette virtuel ou l'unité vFlash et changez la position du périphérique dans la séquence de démarrage. En outre, appuyez sur la barre d'espacement dans la séquence de démarrage dans la configuration CMOS pour rendre le périphérique virtuel amorçable. Par exemple, pour démarrer depuis un lecteur de CD, définissez le lecteur comme premier périphérique dans la séquence de démarrage.

Quels sont les types de supports qui peuvent être définis comme périphériques amorçables ?

iDRAC7 permet de démarrer à partir des supports amorçables suivants :

- Support de données CD-ROM/DVD
- Image ISO 9660
- Disquette 1,44 ou image de disquette
- Clé USB qui est reconnue par le système d'exploitation comme disque amovible
- Image de clé USB

Comment rendre une clé USB amorçable ?

Recherchez l'utilitaire Dell Boot sur le site **support.dell.com**.

Vous pouvez également démarrer avec un disque de démarrage Windows 98 et copier les fichiers système du disque de démarrage vers la clé USB. Par exemple, depuis l'invite DOS, entrez la commande suivante :

```
sys a: x: /s
```

, où x: est la clé USB qui doit être définie comme périphérique amorçable.

Média Virtuel est connecté au lecteur de disquette distant, mais le lecteur de disquette virtuel/CD virtuel est introuvable sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux. Comment résoudre ce problème ?

Certaines versions de Linux ne montent pas automatiquement le lecteur de disquette virtuel et le lecteur de CD virtuel de la même manière. Pour monter le lecteur de disquette virtuel, recherchez le noeud que Linux affecte au lecteur. Pour monter le lecteur :

1. Ouvrez une invite de commande Linux et exécutez la commande suivante :
   `grep "Virtual Floppy" /var/log/messages`
2. Recherchez la dernière entrée de ce message et notez l'heure.
3. Dans l'invite Linux, exécutez la commande suivante :
   `grep "hh:mm:ss" /var/log/messages`

   hh:mm:ss correspond à l'horodatage du message retourné par grep à l'étape 1.
4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom de périphérique attribué au lecteur de disquette virtuel.
5. Vérifiez que vous êtes connecté au lecteur de disquette virtuel.
6. Dans l'invite Linux, exécutez la commande suivante :
   `mount /dev/sdx /mnt/floppy`

   , où `/dev/sdx` est le nom de périphérique trouvé à l'étape 4 et `/mnt/floppy` correspond au point de montage.

Pour monter le lecteur de CD, recherchez le noeud de périphérique que Linux affecte au lecteur. Pour monter le lecteur :

1. Ouvrez une invite de commande Linux et exécutez la commande suivante :
   `grep "Virtual CD" /var/log/messages`
2. Recherchez la dernière entrée de ce message et notez l'heure.
3. Dans l'invite Linux, exécutez la commande suivante :
   `grep "hh:mm:ss" /var/log/messages`

   hh:mm:ss correspond à l'horodatage du message retourné par grep à l'étape 1.
4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom de périphérique affecté au *lecteur de CD virtuel Dell*.
5. Vérifiez que le lecteur de CD virtuel est connecté.
6. Dans l'invite Linux, exécutez la commande suivante :
   `mount /dev/sdx /mnt/CD`

   , où `/dev/sdx` est le nom de périphérique trouvé à l'étape 4 et `/mnt/floppy` correspond au point de montage.

Pourquoi les lecteurs virtuels connectés au serveur sont-ils supprimés après une mise à jour de micrologiciel en utilisant l'interface Web iDRAC7 ?

Les mises à jour micrologicielles provoquent la réinitialisation d'iDRAC7, suppriment la connexion distante et démontent les lecteurs. Les lecteurs réapparaissent à la fin de la réinitialisation d'iDRAC7.

Pourquoi tous les périphériques USB sont-ils déconnectés après la connexion d'un périphérique USB ?

Les périphériques Média Virtuel et les périphériques vFlash sont connectés comme périphériques USB composites au BUS USB hôte et ils partagent un port USB. Lorsque vous connectez un média virtuel ou un périphérique USB vFlash à ce bus ou le déconnectez du bus, tous les médias virtuels et périphériques vFlash sont déconnectés temporairement du bus USB hôte, puis reconnectés. Si le système d'exploitation hôte utilise un périphérique, ne connectez pas ou ne déconnectez pas un ou plusieurs périphériques Média Virtuel ou vFlash. Il est recommandé de connecter tous les périphériques USB nécessaires avant de les utiliser.

Quelle est la fonction du bouton Réinitialisation USB ?

Il réinitialise les périphériques USB distants et locaux connectés au serveur.

Comment optimiser les performances Média Virtuel ?

Lancez Média virtuel avec la console virtuelle désactivée ou procédez de l'une des manières suivantes :

- Amenez le cureur des performances sur la vitesse maximale.
- Désactivez le cryptage pour Média Virtuel et la console virtuelle.

REMARQUE : Dans ce cas, le transfert des données entre le serveur géré et iDRAC7 pour Média Virtuel et la console virtuelle n'est pas sécurisé.

- Si vous utilisez un système d'exploitation Windows, arrêtez le service Windows appelé Collecteur d'événements de Windows. Pour ce faire, accédez à **Démarrer** → **Outils d'administration** → **Services**. Cliquez avec le bouton droit de la souris sur **Collecteur d'événements de Windows** et cliquez sur **Arrêter**.

Lors de la visualisation du contenu d'un lecteur de disquette ou d'une clé USB, un message d'échec de connexion s'affiche si le même lecteur est connecté via Média Virtuel ?

L'accès simultané aux lecteurs de disquette virtuels n'est pas autorisé. Fermez l'application utilisée pour afficher le contenu avant de tenter de virtualiser le lecteur.

Quels types de systèmes de fichiers sont pris en charge sur le lecteur de disquette virtuel ?

Le lecteur de disquette virtuel prend en charge les systèmes de fichiers FAT16 ou FAT32.

Pourquoi un message d'erreur s'affiche lors de la connexion d'un DVD/USB via Média Virtuel, même si le média virtuel n'est pas en cours d'utilisation ?

Ce message s'affiche si la fonction de partage de fichier à distance (RFS) est également utilisée. Vous pouvez utiliser à tout moment RFS ou Média Virtuel, mais pas les deux.

Carte SD vFlash

Quand la carte SD vFlash est-elle verrouillée ?

Elle est verrouillée lorsqu'une opération est en cours, par exemple, pendant une initialisation.

Authentification

Pourquoi le message « Accès distant : échec de l'authentification SNMP »' s'affiche-t-il ?

Lors de la découverte, l'Assistant IT tente de vérifier les noms de communauté get et set du périphérique. L'Assistant IT contient get community name = public et set community name = private. Par défaut le nom de communauté d'agent SNMP pour l'agent iDRAC7 est public. Lorsque l'Assistant IT en voie une demande set, l'agent iDRAC7 génère l'erreur d'authentification SNMP, car il accepte les demandes uniquement de community = public.

Pour éviter les erreurs d'authentification SNMP, vous devez entrer les noms de communauté acceptés par l'agent. Comme iDRAC7 n'autorise qu'un seul nom de communauté, vous devez utiliser le même nom de communauté get et set pour la configuration de découverte de l'Assistant IT.

Périphériques de stockage

Les informations sur tous les périphériques de stockage connectés au système ne sont pas affichées et OpenManage Storage Management affiche plus de périphériques de stockage qu'iDRAC7. Pourquoi ?

iDRAC7 affiche des informations uniquement pour les périphériques pris en charge CEM (Comprehensive Embedded Management).

Interface RACADM

Après avoir réinitialisé iDRAC7 (à l'aide de la commande racadm racreset), le message suivant s'affiche lors de l'exécution d'une commande. Qu'est-ce que cela indique ?

```
ERREUR : impossible de se connecter au RAC à l'adresse IP spécifiée.
```

Le message indique que vous devez attendre qu'iDRAC7 termine la réinitialisation avant d'exécuter une autre commande.

Lorsque vous exécutez des commandes et des sous-commandes RACADM, certaines erreurs ne sont pas effacées.

Une ou plusieurs des erreurs suivantes peuvent survenir lorsque vous utilisez les commandes et les sous-commandes RACADM :

- Messages d'erreur de l'interface locale RACADM : problèmes tels que erreurs de syntaxe, erreurs typographiques et noms incorrects.
- Messages d'erreur de l'interface distante RACADM : problèmes tels que adresse IP incorrecte, nom d'utilisateur incorrect ou mot de passe incorrect.

Au cours d'un test ping vers iDRAC7, si le mode réseau commute entre les modes Dédié et Partagé, vous ne recevez aucune réponse ping.

Effacez la table ARP sur votre système.

L'interface distante RACADM ne parvient pas à se connecter à iDRAC7 à partir de SUSE Linux Enterprise Server (SLES) 11 SP1

Vérifiez que les versions officielles de openssl et libopenssl sont installées. Exécutez la commande suivante pour installer les modules RPM :

```
rpm -ivh --force  <nom de fichier>
```

, où `nom de fichier` correspond au fichier du module rpm openssl ou libopenssl.

Par exemple :

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64 rpm
```

```
rpm -ivh --force libopenssl0_9_8-0.9,8h-30.22.21.1.x86_64.rpm
```

L'interface distante RACADM et les services Web ne sont plus disponibles lorsqu'une propriété est modifiée. Pourquoi ?

Lorsque vous réinitialisez le serveur Web iDRAC7, il peut s'écouler un certain temps avant que les services RACADM et l'interface Web ne redeviennent disponibles.

Le serveur Web iDRAC7 est réinitialisé lorsque :

- Les propriétés de configuration réseau ou de sécurité réseau sont modifiées à l'aide de l'interface utilisateur Web iDRAC7.
- La propriété cfgRacTuneHttpsPort est modifiée (y compris lorsqu'une commande `fichier config` la modifie).
- La commande racresetcfg est utilisée.
- iDRAC7 est réinitialisé.
- Un nouveau certificat de serveur SSL est téléversé.

Pourquoi un message s'affiche lorsque j'essaie de supprimer une partition après l'avoir créée en utilisant l'interface locale RACADM ?

Le message s'affiche, car l'opération de création de partition est en cours. Cependant, la partition est supprimée après un moment et un message indiquant que la partition est supprimée s'affiche. Si tel n'est pas le cas, attendez la fin de la création de la partition et supprimez la partition.

Divers

Comment rechercher l'adresse IP d'iDRAC d'un serveur lame ?

Procédez de l'une des manière suivantes :

Utilisation de l'interface Web CMC : accédez **Châssis → Serveurs → Configuration → Déployer** et dans le tableau qui s'affiche, identifiez l'adresse IP du serveur.

Utilisation de la console virtuelle : redémarrez le serveur pour afficher l'adresse du serveur en utilisant POST. Sélectionnez la console "Dell CMC" dans OSCAR pour vous connecter à CMC via une connexion série locale. Les

commandes CMC RACADM peuvent être envoyées depuis cette connexion. Voir le *Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC* pour la liste complète des sous-commandes CMC RACADM.

Dans l'interface locale RACADM, utilisez la commande `racadm getsysinfo`. Par exemple :

```
$ racadm getniccfg -m server-1 DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet
Mask = 255.255.255.0 Gateway = 192.168.0.1
```

Utilisation de l'écran LCD : dans le menu principal, sélectionnez le serveur, appuyez sur le bouton de vérification, sélectionnez le serveur approprié, puis appuyez sur le bouton de vérification.

Comment rechercher l'adresse IP CMC du serveur lame ?

Interface Web d'iDRAC7 : cliquez **Présentation générale → Paramètres iDRAC → CMC.** La page du **résumé CM** contient l'adresse IP CMC.

Depuis la console virtuelle : sélectionnez la console "Dell CMC" dans OSCAR pour vous connecter à CMC via une connexion série locale. Les commandes CMC RACADM peuvent être émises depuis cette connexion. Voir le *Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC* pour la liste complète des sous-commandes CMC RACADM.

```
$ racadm getniccfg -m chassis NIC Enabled = 1 DHCP Enabled = 1 Static IP
Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway =
192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask =
255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex =
Autonegotiate
```

REMARQUE : Vous pouvez également utiliser ces informations via l'interface distante RACADM.

Comment rechercher l'adresse IP iDRAC IP d'un serveur en rack ou de type tour ?

Interface Web d'iDRAC7 : accédez **Présentation générale → Serveur → Propriétés → Résumé**. La page **Résumé du système** contient l'adresse IP iDRAC7.

Dans l'interface locale RACADM : utilisez la commande `racadm getsysinfo`.

Depuis l'écran LCD : sur le serveur physique, utilisez les boutons de navigation du panneau LCD pour afficher l'adresse IP iDRAC7. Accédez à **Vue Configuration → Vue → Adresse IP iDRAC → IPv4** ou **IPv6 → IP**.

Depuis OpenManage Server Administrator : dans l'interface Web Server Administrator, accédez à **Enceinte modulaire → Système/Module serveur → Châssis du système principal/Système principal → Accès distant**.

La connexion réseau iDRAC7 ne fonctionne pas.

Pour les serveurs lames :

- Vérifiez que le câble LAN est connecté à CMC.
- Vérifiez que les paramètres NIC, les paramètres IPv4 ou IPv6 et que Statique ou DHCP est activé pour votre réseau.

Pour les serveurs en rack et de type tour :

- En mode partagé, vérifiez que le câble LAN est connecté au port NIC où figure le symbole de clé.
- En mode Dédié, vérifiez que le câble LAN est connecté au port LAN iDRAC.
- Vérifiez que les paramètres NIC, les paramètres IPv4 ou IPv6 et que Statique ou DHCP est activé pour votre réseau.

Le serveur lame est inséré dans le châssis, mais l'actionnement du bouton Marche/Arrêt ne met pas le serveur sous tension

- iDRAC7 nécessite deux minutes pour s'initialiser avant la mise sous tension du serveur.
- Vérifiez le budget d'alimentation CMC. Il se peut que le budget d'alimentation du châssis ait été atteint.

Comment extraire le nom et le mot de passe d'un administrateur iDRAC7 ?

Vous devez restaurer les paramètres par défaut d'iDRAC7. Pour plus d'informations, voir Rétablissement des paramètres par défaut définis en usine d'iDRAC7.

Comment changer le nom du logement du système dans un châssis ?

1. Ouvrez une session dans l'interface Web CMC et accédez à **Châssis** → **Serveurs** → **Installation** .
2. Entrez le nouveau nom du logement dans la ligne du serveur et cliquez sur **Appliquer**.

iDRAC7 sur le serveur lame ne répond pas au cours du démarrage.

Retirez et réinsérez le serveur.

Vérifiez l'interface Web CMC pour déterminer si iDRAC7 est indiqué comme composant pouvant être mis à niveau. Si tel est le cas, suivez les instructions dans Mise à niveau du micrologiciel à l'aide de l'interface CMC.

Si le problème persiste, contactez le service de support technique.

Lors de la tentative de démarrage du serveur géré, le voyant d'alimentation est vert, mais aucun POST ou aucune vidéo ne s'affiche.

Ce problème apparaît pour l'une des raisons suivantes :

- La mémoire n'est pas installée ou elle est inaccessible.
- Le processeur n'est pas installé ou il est inaccessible.
- La carte complémentaire vidéo n'est pas installée ou elle n'est pas connectée correctement.

Consultez également les messages d'erreur dans le journal iDRAC7 en utilisant l'interface Web iDRAC7 ou l'écran LCD du serveur.

21

Scénarios de cas d'utilisation

Cette section explique comment accéder à des sections spécifiques du guide pour exécuter des scénarios de cas d'utilisation types.

Dépannage d'un système géré inaccessible

Après avoir reçu des alertes d'OpenManage Essentials, de Dell Management Console ou d'un collecteur d'interruptions local, cinq serveurs dans un centre de données sont inaccessibles suite à un blocage du système d'exploitation ou du serveur. Il est nécessaire d'identifier l'origine du problème et de démarrer le serveur à l'aide d'iDRAC7.

Avant de dépanner le système inaccessible, vérifiez si les conditions suivantes existent :

- Écran du dernier blocage activé
- Les alertes sont activées dans iDRAC7

Pour identifier la cause, vérifiez les éléments suivants dans l'interface Web iDRAC et rétablissez la connexion au système :

REMARQUE : Si vous ne pouvez pas vous connecter à l'interface Web iDRAC, accédez au panneau LCD, notez l'adresse IP ou le nom d'hôte, puis exécutez les opérations suivantes en utilisant l'interface Web d'iDRAC depuis la station de gestion :

- État du voyant du serveur : orange clignotant ou orange fixe.
- État de l'écran LCD du panneau avant : LCD orange ou message d'erreur.
- L'image du système d'exploitation figure dans la console virtuelle. Si vous pouvez voir l'image (démarrage à chaud), ouvrez une nouvelle session. Si vous pouvez ouvrir une session, le problème est résolu.
- Écran du dernier blocage
- Vidéo de capture de démarrage.
- Vidéo de capture de blocage.
- État d'intégrité du serveur : icônes *x* rouges pour les composant défaillants.
- État de la baie de stockage : baie éventuellement hors ligne ou défaillante
- Journal Lifecycle des événements critiques liés au matériel et au micrologiciel du système et entrées de journal consignées lors du blocage du système.
- Générer un rapport de support technique et afficher les données collectées.
- Utiliser les fonctions de surveillance offertes par le module de service iDRAC

Liens connexes

Prévisualisation de la console virtuelle
Affichage des vidéos de capture de démarrage et de blocage
Affichage de l'intégrité du système
Affichage des journaux
Création d'un rapport de support technique
Inventaire et surveillance des périphériques de stockage
Utilisation du module de service iDRAC

Obtention des informations système et évaluation de l'intégrité du système

Pour obtenir les informations système et évaluer l'intégrité du système :

- Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Résumé du système** pour afficher les informations du système et accéder aux liens de la page pour évaluer l'intégrité du système. Par exemple, vous pouvez évaluer l'intégrité du ventilateur du châssis.
- Vous pouvez également configurer le voyant d'emplacement dans le châssis et, en fonction de la couleur, évaluer l'intégrité du système.
- Si le module de service iDRAC est installé, les informations d'hôte du système d'exploitation sont affichées.

Liens connexes

Affichage de l'intégrité du système
Utilisation du module de service iDRAC
Création d'un rapport de support technique

Définition des alertes et configuration des alertes par e-mail

Pour définir des alertes et des alertes par e-mail :

1. Activez les alertes.
2. Configurez l'alerte par e-mail et vérifiez les ports.
3. Redémarrez le système géré, mettez-le hors tension ou exécutez un cycle d'alimentation sur le système géré.
4. Envoyez une alerte de test.

Affichage et exportation du journal Lifecycle et du journal des événements système

Pour afficher et exporter le journal Lifecycle et le journal des événements système (SEL) :

1. Dans l'interface Web iDRAC7, accédez à **Présentation générale** → **Serveur** → **Journaux** pour afficher le journal SEL; et **Présentation générale** → **Serveur** → **Journaux** → **Journal Lifecycle** pour afficher le journal Lifecycle.

   REMARQUE : Le journal est également enregistré dans le journal Lifecycle. Utilisez les options de filtrage pour afficher le journal SEL.
2. Exportez le journal SEL ou Lifecycle au format XML vers un emplacement externe (station de gestion, USB, partage de réseau, etc.). Vous pouvez également activer la journalisation sur un système distant pour que tous les journaux écrits dans le journal Lifecycle soient écrits également simultanément sur le ou les serveurs distants configurés.
3. Si vous utilisez le module de service iDRAC, exportez le journal Lifecycle vers le journal du système d'exploitation. Pour plus d'informations, reportez-vous à la section Utilisation du module de service iDRAC.

Interfaces de mise à niveau du micrologiciel iDRAC

Utilisez les interfaces suivantes pour mettre à jour le micrologiciel iDRAC :

- Interface Web iDRAC7
- CLI RACADM (iDRAC7 et CMC)
- DUP (Dell Update Package)

- Interface Web CMC
- Services à distance Lifecycle Controller
- Lifecycle Controller
- DRACT (Dell Remote Access Configuration Tool)

Exécution d'un arrêt normal

Pour exécuter un arrêt normal, dans l'interface Web d'iDRAC7, accédez aux emplacements suivants :

- **Présentation générale** → **Serveur** → **Alimentation/Thermique** → **Configuration de l'alimentation** → **Contrôle de l'alimentation**. La page **Contrôle de l'alimentation** s'affiche. Sélectionnez **Arrêt normal** et cliquez sur **Appliquer**.
- **Présentation générale** → **Serveur** → **Alimentation/Thermique** → **Surveillance de l'alimentation**. Dans le menu déroulant **contrôle de l'alimentation**, sélectionnez **Arrêt normal**, puis cliquez sur **Appliquer**.

Pour plus d'informations, voir l'*Aide en ligne d'iDRAC7*.

Création d'un compte d'administrateur

Vous pouvez modifier le compte d'administrateur par défaut ou créer un compte d'administrateur. Pour modifier le compte d'administrateur local, voir Modification des paramètres du comptes d'administrateur.

Pour créer un compte d'administrateur, voir les sections suivantes :

- Configuration d'utilisateurs locaux
- Configuration d'utilisateur Active Directory
- Configuration d'utilisateurs LDAP générique

Lancement de la console distante du serveur et montage d'un lecteur USB

Pour lancer la console distante et monter un lecteur USB :

1. Connectez un lecteur Flash USB (avec l'image nécessaire) à la station de gestion.
2. Utilisez les méthodes suivantes pour lancer la console virtuelle via l'interface Web iDRAC7 :
   - Allez à **Présentation générale** → **Serveur** → **Console virtuelle** et cliquez sur **Lancer la console virtuelle**.
   - Accédez à **Présentation générale** → **Serveur** → **Propriétés** et cliquez sur **Lancer** sous **Prévisualisation de la console virtuelle**.

   Le **Visualiseur de console virtuelle** s'affiche.
3. Dans le menu **Fichier**, cliquez sur **Média Virtuel** → **Lancer Média Virtuel** .
4. Cliquez sur **Ajouter une image** et sélectionnez l'image qui se trouve sur le lecteur Flash USB.
   L'image est ajoutée à la liste des lecteurs disponibles.
5. Sélectionnez le lecteur à lui associer. L'image sur le lecteur Flash USB est associée au système géré.

Installation d'un système d'exploitation Bare Metal à l'aide de Média Virtuel connecté et le partage de fichier à distance

Voir Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance.

Gestion de la densité d'un rack

Actuellement, les deux serveurs sont installés dans un rack. Pour ajouter deux serveurs, vous devez déterminer la capacité restante dans le rack.

Pour évaluer la capacité d'un rack pour ajouter des serveurs :

1. Affichez les données de consommation électrique actuelle et l'historique de consommation des serveurs.
2. En fonction des données, de l'infrastructure d'alimentation et des limitations du système, activez la stratégie de limitation de puissance et définissez les valeurs correspondantes.

   REMARQUE : Il est recommandé de définir une limite proche du pic, puis d'utiliser le niveau limité pour déterminer la capacité restante dans le rack pour ajouter des serveurs.

Installation d'une nouvelle licence électronique

Voir Opérations de licence pour plus d'informations.

Application des paramètres de configuration d'identité d'E/S pour plusieurs cartes réseau lors du redémarrage d'un système hôte unique

Si vous disposez de plusieurs cartes réseau dans un serveur qui fait partie d'un environnement SAN (Storage Area Network) et que vous souhaitez leur appliquer différents paramètres d'adresse virtuelle, d'initiateur et de configuration cible, utilisez la fonction d'optimisation d'identité d'E/S pour réduire le temps de configuration des paramètres. Pour ce faire :

1. Assurez-vous que le BIOS, l'iDRAC et les cartes réseau sont mis à jour à la dernière version du micrologiciel.
2. Activez l'optimisation d'identité ES.
3. Exportez le fichier de configuration XML à partir d'iDRAC.
4. Modifiez les paramètres d'optimisation d'identité d'E/S dans le fichier XML.
5. Importez le fichier de configuration XML sur l'iDRAC.

Liens connexes

Mise à jour du micrologiciel de périphérique

Activation ou désactivation de l'optimisation d'identité d'E/S