Guide de l’utilisateur iDRAC10

1.10.xx Series

Décembre 2024
Rév. A00

DELL Technologies

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Historique des révisions

Tableau 1. Historique des révisions

Date	Révision du document	Description des modifications
Décembre 2024	A00	iDRAC10 version 1.10.17.00

Table des matières

1

Présentation de l'iDRAC

Le contrôleur iDRAC (Integrated Dell Remote Access Controller) est conçu pour améliorer la productivité des administrateurs système et la disponibilité générale des serveurs Dell. L'iDRAC signale aux administrateurs les incidents du système, les aide à gérer le système à distance, et réduit les besoins d'accéder physiquement au système.

La technologie de l'iDRAC fait partie d'une large solution de datacenter qui permet d'améliorer la disponibilité des applications et des charges applicatives stratégiques. Cette technologie vous permet de déployer, surveiller, gérer, configurer, mettre à jour et dépanner les systèmes Dell à partir de n'importe quel emplacement et sans l'aide d'aucun agent ou d'un système d'exploitation.

REMARQUE : Il arrive que le comportement de l'iDRAC ne soit pas cohérent lorsqu'il est utilisé avec du matériel non Dell.

Plusieurs produits fonctionnent avec iDRAC pour simplifier et rationaliser les opérations IT. Vous trouverez ci-après la liste répertoriant plusieurs de ces outils :

- OpenManage Enterprise
- Plug-in OpenManage Power Center
- OpenManage Integration for VMware vCenter
- Dell Repository Manager

Il existe les variantes suivantes d'iDRAC :

- IDRAC Core : disponible par défaut sur tous les serveurs
- iDRAC Enterprise : disponible sur tous les modèles de serveur
- iDRAC Datacenter : disponible sur tous les modèles de serveur

Sujets :

Avantages de l'utilisation de l'iDRAC

Avantages :

- Amélioration de la disponibilité : notification anticipée des pannes potentielles ou réelles pour éviter une défaillance d'un serveur ou réduire le délai de reprise après une défaillance.
- Amélioration de la productivité et réduction du coût total TCO : comme les administrateurs peuvent accéder à un plus grand nombre de serveurs distants, le personnel IT est plus productif et les coûts opérationnels, tels que les déplacements, sont réduits.
- Environnement sécurisé : en bénéficiant d'un accès sécurisé aux serveurs distants, les administrateurs peuvent exécuter des fonctions de gestion importantes sans affecter la sécurité des serveurs et du réseau.

Principales fonctionnalités

Les principales fonctionnalités disponibles dans iDRAC sont :

REMARQUE : Certaines fonctionnalités sont disponibles uniquement avec la licence iDRAC Enterprise ou Datacenter. Pour en savoir plus sur les fonctions disponibles avec une licence, voir Fonctionnalités sous licence dans iDRAC10. Pour obtenir la liste des fonctionnalités non prises en charge dans IDRAC10 version 1.10.17.00, reportez-vous à la section Fonctionnalités non prises en charge dans cette version.

Inventaire et surveillance

- Streaming de données de télémétrie.
- Affichage de l'intégrité des serveurs.
- Effectuez l'inventaire et surveillez les adaptateurs de réseau et les sous-systèmes de stockage (PERC et Direct Attached Storage) 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 du processeur, la limitation automatique du processeur et les échecs prédictifs.
- Affichez les informations relatives à la mémoire.
- Surveillance et contrôle de l'utilisation de l'alimentation
- Prise en charge des opérations get SNMPv3 et des alertes.
- Affichez les interfaces réseau disponibles sur les systèmes d'exploitation hôtes.
- IDRAC10 offre de meilleures fonctionnalités de contrôle et de gestion avec Quick Sync 2. L'application OpenManage Mobile doit être configurée sur votre appareil mobile Android ou iOS.

Déploiement

- Gestion des paramètres réseau iDRAC.
- Configuration et utilisation d'une console virtuelle de média virtuel
- Déploiement des systèmes d'exploitation à l'aide du partage de fichiers à distance et du média virtuel.
- Activation de l'auto-détection.
- Apportez des modifications à la configuration du serveur à l'aide de la fonctionnalité de profil de configuration du serveur (SCP). Pour en savoir plus, voir le Guide de référence SCP.
- Configurez la stratégie de persistance des adresses virtuelles, de l'initiateur et des cibles de stockage.
- Configurez à distance les périphériques de stockage reliés au système au moment de l'exécution.
- Effectuez les opérations suivantes pour les périphériques de stockage :
  - Disques physiques : affectez ou annulez l'affectation d'un disque physique comme disque de secours global.
  - Disques virtuels :
    - Créez des disques virtuels.
    - Modifiez les règles de cache des disques virtuels.
    - Vérifiez la cohérence de disque virtuel.
    - Initialisez des disques virtuels.
    - Chiffrez des disques virtuels.
    - Affectez ou annulez l'affectation d'un disque de secours dédié.
    - Supprimez des disques virtuels.
  - Contrôleurs :
    - Configurez les propriétés du contrôleur.
    - Importez ou importez automatiquement la configuration étrangère.
    - Effacez une configuration étrangère.
    - Réinitialisez la configuration du contrôleur.
    - Créez ou modifiez les clés de sécurité.
  - Périphériques SSD PCIe :
    - Faites l'inventaire et surveillez à distance l'intégrité des périphériques SSD PCIe dans le serveur.
    - Préparez le retrait du SSD PCIe.
    - Effacez les données en toute sécurité.
  - Définissez le mode de fond de panier (mode unifié ou divisé).
  - Faites clignoter ou annulez le clignotement des LED des composants.
  - Appliquez les paramètres d'appareil immédiatement, lors du prochain redémarrage du système, à une heure donnée ou comme opération en attente à appliquer en tant que lot dans le cadre de la tâche unique.

Mise à jour

- Gérer les licences iDRAC.
- Mettre à jour le BIOS et le firmware des périphériques pris en charge par le Lifecycle Controller.
- Mettre à jour ou restaurer le firmware iDRAC et le firmware Lifecycle Controller à l'aide d'une seule image de firmware.
- Gérer les mises à jour différées.
- Accédez à l'interface iDRAC via connexion USB directe.
- Configurez l'iDRAC à l'aide des profils de configuration de serveur sur un périphérique USB.

Maintenance et dépannage

- Exécution d'opérations d'alimentation et surveillance de la consommation électrique.
- Optimisez les performances du système et la consommation électrique en modifiant les paramètres thermiques.
- Journalisation des données d'événements : journaux Lifecycle et journaux RAC
- Configuration des alertes par e-mail, alertes IPMI, journaux de système distant, journaux d'événements WS, événements Redfish et interruptions SNMP (v1, v2c et v3) pour des événements et notifications d'alerte par e-mail optimisées.
- Capture de la dernière image de blocage du système
- Affichage des vidéos de capture du démarrage et du blocage.
- Surveillez hors bande et renseignez l'indice de performances sur le processeur, la mémoire et les modules d'E/S.
- Configurez un seuil d'avertissement de la température d'entrée et de la consommation électrique.
- Utilisez l'iDRAC Service Module pour effectuer les opérations suivantes :
  - Affichage des informations sur le système d'exploitation.
  - Réplication des journaux Lifecycle Controller dans les journaux du système d'exploitation.
  - Options de récupération automatique du système.
  - Activez ou désactivez l'état du cycle d'alimentation complet de tous les composants du système, à l'exception du bloc d'alimentation.
  - Hard-reset de l'iDRAC à distance
  - Activez les alertes SNMP intrabande de l'iDRAC.
  - Accédez à l'iDRAC à l'aide du système d'exploitation hôte (fonctionnalité expérimentale).
  - Saisie des informations de l'Infrastructure de gestion Windows (WMI).
  - Intégrez à la collecte SupportAssist. Cela s'applique uniquement si l'iDRAC Service Module version 2.0 ou supérieure est installé.

Les pratiques d'excellence de Dell concernant iDRAC

- Les iDRAC de Dell sont conçus pour figurer sur un réseau de gestion distinct ; ils ne sont pas destinés à être placés sur Internet ou connectés directement à celui-ci. Cette opération risque d'exposer le système connecté à des risques pour la sécurité et autres, pour lesquels Dell n'est pas responsable.
- Dell Technologies recommande d'utiliser le port Gigabit Ethernet dédié disponible sur les serveurs au format rack et les serveurs tours. 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. L'option Dédié permet au contrôleur iDRAC de se voir attribuer une adresse IP du même sous-réseau ou d'un sous-réseau différent par comparaison aux adresses IP affectées au LOM ou aux cartes réseau hôtes.
- En plus de placer les DRAC sur un sous-réseau de gestion distinct, les utilisateurs doivent isoler le vLAN/sous-réseau de gestion avec des technologies telles que des pare-feux, et limiter l'accès au sous-réseau/vLAN aux administrateurs de serveur autorisés.

Sécurisation des connexions

Sécuriser l'accès aux ressources réseau stratégiques étant une priorité, l'iDRAC met en œuvre une série de fonctionnalités de sécurité, notamment :

- Certificat de signature personnalisé pour le certificat SSL (couche de sockets sécurisée).
- Mises à jour du firmware signé
- Authentification utilisateur via Microsoft Active Directory, protocole LDAP (Lightweight Directory Access Protocol) générique, ou ID et mots de passe utilisateur administrés localement.
- Authentification à deux facteurs à l'aide de la fonctionnalité de connexion par carte à puce. Cette authentification repose sur la carte à puce physique et son code PIN.
- Authentification unique et authentification par clé publique.
- Autorisation basée sur le rôle pour définir des privilèges pour chaque utilisateur
- Authentification SNMPv3 pour les comptes utilisateur stockés localement dans l'iDRAC. Il est recommandé de l'utiliser, mais elle est désactivée par défaut.
- Configuration de l'ID utilisateur et du mot de passe
- Modification du mot de passe d'ouverture de session par défaut.
- Définissez les mots de passe utilisateur et les mots de passe du BIOS en utilisant un format chiffré unidirectionnel pour une sécurité renforcée.

- Fonctionnalité FIPS 140-2 de niveau 1.
- Configuration du délai d'expiration de la session (en secondes)
- Ports IP configurables (pour HTTP, HTTPS, SSH, Console virtuelle et Média virtuel).
- SHH (Secure Shell) qui utilise une couche de transport chiffrée pour une sécurité accrue.
- Nombre maximal d'échecs de la 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 iDRAC.
- Adaptateur de la carte Gigabit Ethernet dédiée disponible sur les serveurs en rack et de type tour (du matériel supplémentaire peut être requis).

Nouvelles fonctionnalités ajoutées

Cette section répertorie les nouvelles fonctionnalités ajoutées dans chaque version d'iDRAC10.

Version 1.10.17.00 du firmware

Dans la version iDRAC10 1.10.17.00, les fonctionnalités suivantes sont ajoutées dans l'iDRAC :

- Sécurité renforcée avec un processeur de sécurité dédié :
  - Amélioration des performances de sécurité
  - Root-of-Trust intégré, attestation au niveau de l'appareil et chiffrement
  - Algorithmes de chiffrement renforcés
- Mise à jour de l'interface utilisateur :
  - Expérience utilisateur cohérente sur toutes les consoles Dell technologies
  - Interface simplifiée
  - Navigation simplifiée
- Licence simplifiée dans PowerEdge de 17e génération
- Créer des rôles d'utilisateur iDRAC personnalisés
- Récupération de l'alimentation CA contrôlée par l'iDRAC (le BIOS des générations précédentes gérait ce paramètre)

Fonctions supprimées

Les fonctions suivantes sont comprises dans iDRAC10 :

- Gestionnaire de groupe
- WS-Man
- TLS 1,1
- vFlash

Fonctionnalités non prises en charge dans cette version initiale de l'iDRAC10

Les fonctionnalités suivantes ne sont pas prises en charge dans les versions 1.1x du firmware iDRAC10.

Tableau 2. Fonctionnalités non prises en charge

Fonction	Fonctionnalité
Interface utilisateur iDRAC	Prise en charge d'autres langues par l'interface graphique d'iDRAC.
	RACADM locale (OS intrabande)
	Interface RACADM distante
	Outils du contrôleur iDRAC
	Série - RAC série

Tableau 2. Fonctionnalités non prises en charge (suite)

Fonction	Fonctionnalité
	UI de Lifecycle Controller
	Série - IPMI série
REMARQUE : CLI RACADM accessible via l'interface SSH.	
Mise en réseau et connectivité	Blocage d'adresse IP
	Plage d'IP
	Configuration SCP d'iDRAC Direct (USB)
	Quick Sync
	Vue de la connexion réseau
Gestion à distance	Série sur LAN avec SSH
	Dossiers virtuels
	Partage de fichier à distance
	Contrôle de la qualité/bande passante
	Collaboration de console virtuelle (jusqu'à six utilisateurs simultanés)
	Chat de la console virtuelle
	Presse-papiers virtuel
	Suivi de l'actif
	Suivi d'utilisation du marché (MUT)
	Kit de développement logiciel (SDK)
	Média virtuel : session unique
iDRAC Service Module (iSM)	Réinitialisation matérielle de l'iDRAC et autres fonctionnalités
	Network Information
	IBIA
	Cycle d'alimentation virtuel
	Préparation à la suppression
	SSO iDRAC
	Détails du système d'exploitation
	Surveillance SATA du chipset
	RAID logiciel
	Réplication du journal Lifecycle Controller
	SNMP intrabande
	Intégration de Support Assist
	Relation commune d'événement SDS
	Installation de l'iSM
Alertes	Événements du cycle de vie Redfish (RLCE)
	Syslog distant : non sécurisé
	Syslog distant : sécurisé

Tableau 2. Fonctionnalités non prises en charge (suite)

Fonction	Fonctionnalité
	Télémétrie : streaming
	Télémétrie : rapports de mesures
	Déclencheurs de télémétrie
	Fonctionnalités iSM OS Metric Injection pour la télémétrie
Gestion de la plateforme	SDPM de la mémoire
	NVDIMM de la mémoire
	Surveillance des performances hors bande
	Détection des serveurs inactifs
	Refroidissement liquide
Alimentation et Thermique	Limitation de l'alimentation
	Surveillance de l'alimentation : mesure de l'alimentation en temps réel
	Graphique d'alimentation en temps réel
	Compteurs d'alimentation historiques
	Intégration du plug-in OME Power manager
	Limite de courant d'entrée
	Fresh Air
	ASHERE
	Température d'échappement personnalisée
	Graphiques de température
	Soundcap 1.0
	Consommation de circulation d'air système, température d'entrée PCIe personnalisée
	Personnalisation de la circulation d'air PCIe
Gestion du stockage	Gestion des boîtiers externes
	Secure Enterprise Key Manager (SEKM) et gestion des clés locales de l'iDRAC (iLKM)
	HBA : inventaire et surveillance en temps réel
	HBA : inventaire par étapes
Gestion des communications	DPU : inventaire, surveillance et configuration en temps réel
	DPU : inventaire et configuration par étapes
	Gestion des adresses virtuelles
	Fonctionnalités DPU/SmartNIC
	FC : inventaire et surveillance en temps réel
	FC : inventaire et configuration par étapes
Gestion des accélérateurs	FPGA : inventaire par étapes
	FGPA : inventaire, alimentation et température en temps réel
Déploiement/Configuration de serveur	Pack de pilotes

Tableau 2. Fonctionnalités non prises en charge (suite)

Fonction	Fonctionnalité
	Profil de configuration du serveur : mise à jour du référentiel
	Profil de configuration du serveur : déploiement du système d'exploitation
	Configuration locale
	Configuration sans intervention
Mise à jour du système	Mise à jour du catalogue
	Outils de mise à jour intégrés
	Mise à jour automatique
Usine, diagnostics, service et journalisation	Restauration des valeurs par défaut d'iDRAC
	Secure Erase
	Vidéo d'écran de blocage : avec agent
	Capture d'écran de blocage
	Journal de données série
	Capture vidéo de blocage : sans agent
	Notes de travail
	Syslog distant pour les alertes
Authentification et autorisation	Utilisateur local : compte réservé
	Services d'annuaire
	Active Directory : schéma standard
	Active Directory : schéma étendu
	Authentification unique (SSO)
	Authentification à deux facteurs (2FA) : carte à puce
	Authentification à deux facteurs (2FA) : simple
	Secure Shell Public Key Authentication (SSH PKA)
	RSA Multi-Factor Authentication (RSA MFA)
	OAuth
	OpenID Connect
Sécurité	Certificat SSL : certificat de signature personnalisé
	Certificat SSL : inscription automatique du certificat
	FIPS 140-2/140-3
	Politique de sécurité personnalisée
	Protection contre le blocage d'adresses IP et le déni de service (DOS)
	Sécurité supplémentaire QuickSync 2.0
	Mode de verrouillage du système
	Filtrage de la plage d'adresses IP
	Chaîne chiffrée personnalisée
	Configuration locale

Tableau 2. Fonctionnalités non prises en charge (suite)

Fonction	Fonctionnalité
	Réseau iDRAC : sécurité 802.1x
	BIOS Livescan
Gestion thermique	Personnalisation de la circulation d'air PCIe (LFM)
	Contrôle d'évacuation personnalisé
	Contrôle personnalisé delta-T
	Température d'entrée PCIe personnalisée
	Consommation de débit du système
Autre	ICA adaptative

Comment utiliser ce guide

Instructions utilisateur

Le contenu du présent Guide de l'utilisateur permet d'exécuter diverses tâches à l'aide de :

1. L'interface Web iDRAC : seules les informations liées aux tâches sont fournies ici. Pour plus d'informations sur les champs et les options, voir l'**Aide en ligne d'iDRAC** à laquelle vous pouvez accéder depuis l'interface Web.
2. RACADM : la commande RACADM ou l'objet que vous devez utiliser est indiqué ici. Pour plus d'informations, voir le **Guide de l'interface de ligne de commande RACADM d'iDRAC10** disponible sur le site de support.
3. L'utilitaire de configuration iDRAC : seules les informations liées aux tâches sont fournies ici. Pour plus d'informations concernant les champs et les options, voir l'**Aide en ligne de l'utilitaire de configuration de l'iDRAC**, accessible en cliquant sur **Aide** dans l'interface de configuration de l'iDRAC (appuyez sur <F2> lors du démarrage, puis cliquez sur **Paramètres iDRAC** dans la page **Menu principal de configuration du système**).
4. Reddish : seules les informations liées aux tâches sont fournies ici. Pour plus d'informations sur les champs et les options, consultez le **guide de l'API Redfish iDRAC10** sur le portail des développeurs.

Navigateurs Web pris en charge

Pour obtenir la liste des versions prises en charge, consultez les **Notes de mise à jour de l'iDRAC10** sur le site de support Dell.

Systèmes d'exploitation et hyperviseurs pris en charge

Pour obtenir la liste des versions prises en charge des systèmes d'exploitation et des hyperviseurs, consultez les **Notes de mise à jour de l'iDRAC10** sur le site de support Dell.

Licences iDRAC

Les fonctionnalités iDRAC sont disponibles en fonction du type de licence. La licence iDRAC Core est installée par défaut. La licence iDRAC Enterprise est disponible sous forme de mise à niveau et peut être achetée à tout moment. Seules les fonctionnalités sous licence sont disponibles dans les interfaces qui permettent de configurer ou d'utiliser l'iDRAC. Pour plus d'informations, voir Fonctionnalités sous licence dans iDRAC10.

Types de licences

La licence standard iDRAC est disponible par défaut sur votre système. IDRAC Enterprise et les licences Datacenter incluent toutes les fonctionnalités sous licence et peuvent être achetées à tout moment. Les types de licences proposés en montée de gamme sont les suivants :

- 30 jours d'évaluation : les licences d'évaluation reposent sur la durée et le temps est décompté dès que le système est mis sous tension. Cette licence ne peut pas être prolongée.
- Perpétuelle : la licence est liée à l'étiquette de service et elle est permanente.

Le tableau ci-dessous répertorie les licences par défaut disponibles sur les systèmes :

Tableau 3. Licences par défaut

Licence principale iDRAC	Licence iDRAC Enterprise	Licence iDRAC Datacenter
• Disponible pour tous les serveurs • Fonctionnalités de gestion des systèmes principaux.	• Disponible sous forme de montée de gamme sur tous les serveurs • Fonctionnalités de base, d'automatisation, de console virtuelle et de sécurité. • Fourni avec les licences Secure Enterprise Key Management (SEKM) et Secure Component Verification (SCV).	• Disponible sous forme de montée de gamme sur tous les serveurs • Inclut toutes les fonctionnalités Core et Enterprise. • Inclut des fonctions clés telles que la télémétrie et la gestion thermique. • Inclut des accélérateurs avancés (processeur graphique et DPU), la gestion des systèmes et un refroidissement avancé par air et liquide.

Méthodes d'acquisition de licences

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

- Dell Digital Locker : le service Dell Digital Locker vous permet d'afficher et de gérer vos produits, logiciels et informations relatives aux licences depuis un seul et même emplacement. Un lien d'accès au service Dell Digital Locker est disponible sur l'interface Web du contrôleur DRAC. Accédez à **Configuration** > **Licences**.

REMARQUE : Pour en savoir plus sur le service Dell Digital Locker, reportez-vous à la FAQ sur le site Web.

- E-mail : la licence est jointe à un e-mail envoyé après sa demande auprès du centre de support technique.
- Point de vente : la licence est acquise lors de la commande d'un système.

REMARQUE : Pour gérer les licences ou en acheter de nouvelles, rendez-vous sur le service Dell Digital Locker.

Obtention de la clé de licence à partir de Dell Digital Locker

Pour obtenir la clé de licence depuis votre compte, vous devez d'abord enregistrer votre produit à l'aide du code d'enregistrement qui est envoyé dans l'e-mail de confirmation de commande. Vous devez saisir ce code dans l'onglet **Enregistrement du produit** une fois que vous êtes connecté à votre compte Dell Digital Locker.

Dans le volet de gauche, cliquez sur l'onglet **Produits** ou **Historique des commandes** pour afficher la liste de vos produits. Les produits basés sur un abonnement sont répertoriés sous l'onglet **Comptes de facturation**.

Pour télécharger la clé de licence à partir de votre compte Dell Digital Locker :

1. Connectez-vous à votre compte Dell Digital Locker.
2. Dans le volet de gauche, cliquez sur **Produits**.
3. Cliquez sur le produit que vous souhaitez afficher.
4. Cliquez sur le nom du produit.
5. Sur la page **Gestion de produit**, cliquez sur **Obtenir la clé**.
6. Suivez les instructions qui s'affichent pour obtenir la clé de licence.

REMARQUE : Si vous ne disposez pas d'un compte Dell Digital Locker, créez un compte à l'aide de l'adresse e-mail fournie lors de votre achat.

REMARQUE : Pour générer plusieurs clés de licence pour de nouveaux achats, suivez les instructions sous **Outils** > **Licence d'activation** > **Licences non activées**.

Opérations de licence

Avant d'exécuter les tâches de gestion des licences, veillez à obtenir les licences. Pour plus d'informations, voir les méthodes d'acquisition de licences.

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 iDRAC, RACADM, Redfish 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 iDRAC en utilisant l'une des interfaces prises en charge. La licence est importée si les vérifications de validation auxquelles elle est soumise aboutissent.

  REMARQUE : Bien que vous puissiez exporter la licence installée en usine, vous ne pourrez pas l'importer. Pour importer la licence, téléchargez la licence équivalente du service Digital Locker ou récupérez-la dans l'e-mail d'achat de la licence.

- Exporter : permet d'exporter la licence installée. Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.
- Supprimer : permet de supprimer la licence. Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.
- 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 en savoir plus, voir l'aide d'Internet Explorer.

Vous trouverez ci-dessous les exigences en matière de privilèges utilisateur pour différentes opérations de licence :

- Vue et exportation de licence : privilège de connexion.
- Importation et suppression de licence : privilège de connexion + configuration iDRAC + contrôle du serveur.

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

Gestion des licences

1. Pour gérer les licences à l'aide de l'interface RACADM, utilisez la sous-commande **license**.
2. Pour plus d'informations, consultez Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller

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

Pour gérer les licences à l'aide de l'interface Web de l'iDRAC, accédez à **Configuration** > **Licences**.

La page **Gestion des licences** affiche les licences associées à des appareils ou les licences installées des périphériques non présents dans le système. Pour plus d'informations sur l'importation, l'exportation ou la suppression d'une licence, consultez l'**aide en ligne de l'iDRAC**.

Fonctionnalités sous licence dans iDRAC10

Le tableau suivant répertorie les fonctionnalités iDRAC10 qui sont activées en fonction de la licence achetée :

Tableau 4. Fonctionnalités sous licence dans iDRAC10

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Interfaces et normes			
API RESTful du contrôleur iDRAC et Redfish	Oui	Oui	Oui
IPMI 2,0	Oui	Oui	Oui
DCMI 1,5	Oui	Oui	Oui
IUG web	Oui	Oui	Oui

Tableau 4. Fonctionnalités sous licence dans iDRAC10 (suite)

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Ligne de commande racadm (local/à distance)	Oui	Oui	Oui
SSH	Oui	Oui	Oui
Redirection série	Oui	Oui	Oui
NTP (Network Time Protocol)	Oui	Oui	Oui
Connectivité			
Carte d'interface réseau partagée (LOM)	Oui	Oui	Oui
NIC dédié	Oui	Oui	Oui
Balisage VLAN	Oui	Oui	Oui
IPv4	Oui	Oui	Oui
IPv6	Oui	Oui	Oui
DHCP	Oui	Oui	Oui
DHCP sans intervention	Non	Oui	Oui
DNS dynamique	Oui	Oui	Oui
Connexion directe de l'OS	Oui	Oui	Oui
iDRAC – connexion USB directe sur le panneau avant	Oui	Oui	Oui
Vue de connexion	Oui	Oui	Oui
DPU	Non	Oui	Oui
Sécurité			
Autorité basée sur les rôles	Oui	Oui	Oui
Utilisateurs locaux	Oui	Oui	Oui
Chiffrement SSL	Oui	Oui	Oui
Gestion des clés d'entreprise sécurisées et gestionnaire iDRAC de clés locales	Non	Oui (avec licence SEKM)	Oui (avec licence SEKM)
Blocage d'adresses IP	Non	Oui	Oui
Services de répertoire (AD, LDAP)	Non	Oui	Oui
L'authentification à deux facteurs (carte à puce)	Non	Oui	Oui
Authentification unique	Non	Oui	Oui
Authentification PK (pour SSH)	Oui	Oui	Oui
Intégration OAuth avec des services d'authentification Web	Non	Non	Oui
Contrôle d'accès au réseau basé sur les ports (IEEE 802.1x)	Non	Non	Oui
OpenID Connect pour les consoles Dell	Non	Non	Oui
FIPS 140-2	Oui	Oui	Oui

Tableau 4. Fonctionnalités sous licence dans iDRAC10 (suite)

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Démarrage sécurisé UEFI – gestion des certificats	Oui	Oui	Oui
Verrouillage du système	Non	Oui	Oui
Mot de passe iDRAC par défaut unique	Oui	Oui	Oui
Bannière de stratégie de sécurité personnalisable – page de connexion	Oui	Oui	Oui
Authentification multifacteur facile	Non	Oui	Oui
Inscription automatique de certificat (certificats SSL)	Non	Non	Oui
iDRAC Quick Sync 2 – authentification en option pour les opérations de lecture	Oui	Oui	Oui
iDRAC Quick Sync 2 – ajout d'un numéro d'appareil mobile à LCL	Oui	Oui	Oui
Secure Erase	Oui	Oui	Oui
Analyse du BIOS en temps réel	Non	Oui	Oui
Inscription automatique de certificats SSL	Non	Oui	Oui
Authentification à deux facteurs RSA SecureID (2FA)	Non	Oui	Oui
Périphériques avec RoT	Oui	Oui	Oui
Détection des intrusions	Oui	Oui	Oui
Contrôle d'accès USB	Oui	Oui	Oui
Vérification des composants sécurisés	Non	Oui	Oui
Présence à distance			
Bouton d'alimentation	Oui	Oui	Oui
Contrôle de l'amorçage	Oui	Oui	Oui
Série sur LAN	Oui	Oui	Oui
Support virtuel	Non	Oui	Oui
Dossiers virtuels	Non	Oui	Oui
Partage de fichier à distance	Non	Oui	Oui
Accès HTML5 à la console virtuelle	Non	Oui	Oui
Console virtuelle	Non	Oui	Oui
Presse-papiers virtuel	Non	Oui	Oui
Connexion VNC à l'OS	Non	Oui	Oui
Contrôle de la qualité/bande passante	Non	Oui	Oui

Tableau 4. Fonctionnalités sous licence dans iDRAC10 (suite)

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Collaboration de console virtuelle (jusqu'à six utilisateurs simultanés)	Non	Oui	Oui
Chat de la console virtuelle	Non	Oui	Oui
Prise en charge des protocoles HTTP/HTTPS et NFS/CIFS	Oui	Oui	Oui
Alimentation et Thermique			
Système de gestion thermique avancé	Non	Oui	Oui
Mesure d'énergie en temps réel	Oui	Oui	Oui
Seuils et alertes d'alimentation	Oui	Oui	Oui
Graphique d'alimentation en temps réel	Non	Oui	Oui
Compteurs d'alimentation historiques	Non	Oui	Oui
Limitation de l'alimentation	Non	Oui	Oui
Intégration de Power Center	Non	Oui	Oui
Graphiques de température	Oui	Oui	Oui
Personnalisation de la circulation d'air PCIe (LFM)	Non	Oui	Oui
Contrôle d'évacuation personnalisé	Non	Oui	Oui
Contrôle personnalisé delta-T	Non	Oui	Oui
Consommation de circulation d'air du système	Non	Oui	Oui
Température d'entrée PCIe personnalisée	Non	Oui	Oui
Intégrité			
Surveillance sans agent complète	Oui	Oui	Oui
Surveillance de la température	Oui	Oui	Oui
Surveillance de panne prédictive	Oui	Oui	Oui
SNMP v1, v2 et v3 (interruptions et gets)	Oui	Oui	Oui
Alertes par e-mail	Non	Oui	Oui
Seuils configurables	Oui	Oui	Oui
Surveillance du ventilateur	Oui	Oui	Oui
Surveillance des blocs d'alimentation	Oui	Oui	Oui
Surveillance de la mémoire	Oui	Oui	Oui
Processeur graphique	Non	Oui	Oui
Surveillance de l'UC	Oui	Oui	Oui

Tableau 4. Fonctionnalités sous licence dans iDRAC10 (suite)

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Détection de fuite au niveau du processeur et du processeur graphique	Oui	Oui	Oui
Contrôleurs de stockage	Oui	Oui	Oui
Surveillance de NIC	Oui	Oui	Oui
Inventaire optique	Oui	Oui	Oui
Statistiques optiques	Non	Non	Oui
Surveillance du disque dur	Oui	Oui	Oui
Surveillance des performances hors bande	Non	Oui	Oui
Alertes en cas d'usure excessive des SSD	Oui	Oui	Oui
Paramètres personnalisables pour la température de sortie	Oui	Oui	Oui
Journaux de données série	Non	Oui	Oui
Journaux intelligents pour les disques de stockage	Non	Oui	Oui
Détection de serveur inactif	Non	Oui	Oui
Télémétrie	Non	Oui	Oui
Intégrité cumulée	Oui	Oui	Oui
Mise à jour			
Mise à jour sans agent à distance	Oui	Oui	Oui
Outils de mise à jour intégrés	Oui	Oui	Oui
Mise à jour à partir du référentiel	Oui	Oui	Oui
Mise à jour à partir du référentiel (mise à jour automatique)	Oui	Oui	Oui
Mises à jour du firmware	Oui	Oui	Oui
Déploiement et configuration			
Configuration locale via F2	Non	Oui	Oui
Outils intégrés de déploiement de l'OS	Oui	Oui	Oui
Outils de configuration intégrés	Oui	Oui	Oui
Détection automatique	Non	Oui	Oui
Déploiement de l'OS à distance	Non	Oui	Oui
Pack de pilotes intégré	Oui	Oui	Oui
Inventaire de configuration complet	Oui	Oui	Oui
Exportation de l'inventaire	Oui	Oui	Oui
Configuration à distance	Oui	Oui	Oui
Configuration sans intervention	Non	Oui	Oui

Tableau 4. Fonctionnalités sous licence dans iDRAC10 (suite)

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Mise au retrait ou recyclage du système	Oui	Oui	Oui
Exportation du profil de configuration du serveur	Oui	Oui	Oui
Importation du profil de configuration du serveur	Non	Oui	Oui
Prévisualisation du profil de configuration du serveur	Oui	Oui	Oui
Configuration BIOS	Oui	Oui	Oui
Configuration du stockage	Non	Oui	Oui
Diagnostics, Service et Journalisation			
Suivi de l'actif	Oui	Oui	Oui
Outils de diagnostic intégrés	Oui	Oui	Oui
Remplacement de pièce	Oui	Oui	Oui
Restauration facile (configuration du système)	Oui	Oui	Oui
Voyants d'état d'intégrité	Oui	Oui	Oui
iDRAC Quick Sync 2 (matériel BLE/Wi-Fi)	Oui	Oui	Oui
iDRAC direct (port de gestion USB à l'avant)	Oui	Oui	Oui
iDRAC Service Module (iSM) intégré	Oui	Oui	Oui
Transfert des alertes iSM à intrabande vers les consoles	Oui	Oui	Oui
Collecte SupportAssist (intégré)	Oui	Oui	Oui
Capture d'écran de blocage	Oui	Oui	Oui
Capture vidéo de blocage	Non	Oui	Oui
Capture vidéo en cas de panne sans agent (Windows uniquement)	Non	Non	Oui
Capture à l'amorçage	Oui	Oui	Oui
Réinitialisation à distance pour iDRAC (nécessite iSM)	Oui	Oui	Oui
NMI virtuel	Oui	Oui	Oui
2FA	Non	Oui	Oui
Inventaire et surveillance des périphériques	Oui	Oui	Oui
Notes de travail	Oui	Oui	Oui
Surveillance de l'OS	Oui	Oui	Oui
Journal des événements système	Oui	Oui	Oui
Journal Lifecycle	Oui	Oui	Oui

Tableau 4. Fonctionnalités sous licence dans iDRAC10 (suite)

Fonctionnalité	IDRAC 10 Core	iDRAC 10 Enterprise	IDRAC 10 Datacenter
Amélioration de la consignation dans le journal Lifecycle Controller	Oui	Oui	Oui
Syslog distant	Non	Oui	Oui

REMARQUE : Pour obtenir la liste des fonctionnalités qui ne sont pas prises en charge dans cette version, reportez-vous à la section Fonctionnalités non prises en charge dans cette version

Interfaces et protocoles d'accès à iDRAC

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

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

Tableau 5. Interfaces et protocoles d'accès à iDRAC

Interface ou protocole	Description
Utilitaire de configuration iDRAC (F2)	Utilisez l'utilitaire de configuration iDRAC pour effectuer des opérations en amont du système d'exploitation. Il propose certaines des fonctionnalités de l'interface Web de l'iDRAC, ainsi que d'autres fonctionnalités. Pour accéder à l'utilitaire de configuration de l'iDRAC, appuyez sur <F2> au démarrage, puis cliquez sur **Paramètres iDRAC** sur la page **Menu principal de configuration système**.
Interface web iDRAC	Utilisez l'interface Web iDRAC pour gérer iDRAC et surveiller le système géré. Le navigateur se connecte au serveur Web via le port HTTPS. Les flux de données sont chiffrés avec SSL 128 bits pour garantir leur confidentialité et leur intégrité. Toute connexion au port HTTP est redirigée vers HTTPS. Les administrateurs peuvent importer leur propre certificat SSL en faisant une demande CSR SSL pour sécuriser le serveur Web. Les ports HTTP et HTTPS par défaut peuvent être modifiés. L'accès utilisateur est basé sur des privilèges.
RACADM	Utilisez cet utilitaire de ligne de commande pour gérer iDRAC et le serveur. Vous pouvez utiliser RACADM en local et à distance. ● L'interface de ligne de commande locale RACADM est exécutée sur les systèmes gérés disposant de Server Administrator. L'interface locale RACADM communique avec iDRAC via son interface hôte IPMI intrabande. Étant donné que cet utilitaire est installé sur le système géré local, les utilisateurs doivent se connecter au système d'exploitation pour l'exécuter. Un utilisateur doit disposer de privilèges d'administration complets ou être un utilisateur root pour se servir de cet 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. ● L'interface RACADM du firmware est accessible en se connectant à l'iDRAC via SSH. Vous pouvez exécuter les commandes de cette interface sans spécifier l'adresse IP, le nom d'utilisateur ni le mot de passe iDRAC. ● Vous n'avez pas besoin de spécifier l'adresse IP, le nom d'utilisateur ni le mot de passe iDRAC pour exécuter les commandes de l'interface RACADM du firmware. Une fois que vous êtes entré dans l'invite RACADM, vous pouvez exécuter directement les commandes sans le préfixe racadm.
API RESTful du contrôleur iDRAC et Redfish	L'API Redfish Scalable Platforms Management est une norme définie par l'organisme Distributed Management Task Force (DMTF). Redfish est une norme d'interface de gestion de système de nouvelle génération, qui permet de gérer les serveurs de manière évolutive, sécurisée et ouverte. Cette nouvelle interface utilise la sémantique RESTful pour accéder aux données qui sont définies dans un format de modèle, pour effectuer une gestion des systèmes hors bande. Elle est adaptée à une large gamme de serveurs : serveurs autonomes, environnements rack ou encore environnements Cloud à grande échelle. Redfish offre les avantages suivants par rapport aux méthodes de gestion de serveur existantes : ● Plus de simplicité et une facilité d'utilisation ● Sécurité renforcée des données ● Interface programmable et possibilité de rédiger des scripts facilement. ● Conformité avec les normes les plus courantes. Voir le guide des API Redfish de l'iDRAC.

Tableau 5. Interfaces et protocoles d'accès à iDRAC (suite)

Interface ou protocole	Description
Port USB Type-C	Accédez à l'iDRAC à l'aide du port USB type-C étiqueté.
SSH	Utilisez SSH pour exécuter des commandes RACADM ou démarrer une session de redirection de console. Le service SSH est activé par défaut dans iDRAC. Le service SSH peut être désactivé dans l'iDRAC. L'iDRAC prend uniquement en charge SSH version 2 avec l'algorithme de clé hôte RSA. Une clé d'hôte RSA unique à 1 024 bits est générée lorsque vous allumez iDRAC pour la première fois.
IPMItool	Utilisez IPMITool pour accéder aux fonctionnalités de gestion de base du système distant via iDRAC. L'interface comprend les technologies IPMI local, IPMI sur LAN, IPMI sur série et série sur LAN. Pour plus d'informations sur IPMITool, consultez le **Guide de l'utilisateur des utilitaires Dell OpenManage Baseboard Management Controller**. **REMARQUE :** IPMI version 1.5 n'est pas prise en charge.
NTLM	iDRAC autorise NTLM à des fins d'authentification, d'intégrity et de confidentialité pour les utilisateurs. NT LAN Manager (NTLM) est une suite de protocoles de sécurité Microsoft, compatible avec un réseau Windows.
SMB	L'iDRAC prend en charge le protocole Server Message Block (SMB). Il s'agit d'un protocole de partage de fichiers réseau. Les versions allant de 2.0 à 3.11 de SMB sont prises en charge. SMBv1 n'est plus pris en charge.
NFS	L'iDRAC prend en charge Network File System (NFS). Il s'agit d'un protocole de système de fichiers distribué permettant aux utilisateurs de monter des répertoires à distance sur les serveurs.
TFTP	L'iDRAC utilise le protocole TFTP (Trivial File Transfer Protocol) pour les mises à jour de firmware et les installations de certificats.
CIFS	L'iDRAC utilise le protocole CIFS (Common Internet File System) pour partager des fichiers à distance. CIFS permet de monter des fichiers image ISO ou IMG provenant d'un partage réseau sur le système d'exploitation du serveur géré, en tant que disques virtuels.
HTTP et HTTPS	L'iDRAC prend en charge les protocoles HTTP (Hyper-Text Transfer Protocol) et HTTPS (Hyper-Text Transfer Protocol Secure) pour la gestion à distance des serveurs Dell.

Informations sur les ports iDRAC

Le tableau suivant répertorie les ports qui sont requis pour accéder à distance à iDRAC via un pare-feu. Il s'agit des ports par défaut sur lesquels iDRAC écoute les connexions. Vous pouvez modifier la plupart de ces ports (facultatif). Pour modifier les ports, reportez-vous à la section Services de configuration.

Tableau 6. Ports qu'écoute iDRAC pour les connexions

Numéro de port	Type	Fonction	Ports configurables	Niveau de chiffrement maximal
22	TCP	SSH	Oui	SSL 256 bits
80	TCP	HTTP	Oui	Aucun
161	UDP	Agent SNMP	Oui	Aucun
443	TCP	HTTPS	Oui	SSL 256 bits
623	UDP	RMCP/RMCP+	Non	SSL 128 bits
5000	TCP	iDRAC vers iSM	Non	SSL 256 bits
5901	TCP	VNC	Oui	SSL 128 bits
REMARQUE : Le port 5901 s'ouvre lorsque la fonction VNC est activée.				

Le tableau suivant répertorie les ports qu'iDRAC utilise en tant que client :

Tableau 7. Ports qu'iDRAC utilise comme client

Numéro de port	Type	Fonction	Ports configurables	Niveau de chiffrement maximal
25	TCP	SMTP	Oui	Aucun
53	UDP	DNS	Non	Aucun
68	UDP	Adresse IP attribuée à DHCP	Non	Aucun
69	TFTP	TFTP	Non	Aucun
123	UDP	NTP (Network Time Protocol)	Non	Aucun
162	UDP	Trap SNMP	Oui	Aucun
445	TCP	CIFS (Common Internet File System)	Non	Aucun
636	TCP	LDAP sur SSL (LDAPS)	Non	SSL 256 bits
2049	TCP	NFS (Network File System)	Non	Aucun
3269	TCP	LDAPS pour catalogue global (GC)	Non	SSL 256 bits
5353	UDP	mDNS	Non	Aucun
514	UDP	Syslog distant	Oui	Aucun

Autres documents utiles

L'interface utilisateur de l'iDRAC prend en charge l'**Aide en ligne** intégrée, accessible en cliquant sur l'onglet **Aide et commentaires**. L'**Aide en ligne** présente des informations détaillées sur les champs disponibles dans l'interface Web, ainsi que leurs descriptions. En outre, les documents suivants disponibles sur le site Web de support Dell à l'adresse **dell.com/support** fournissent des informations supplémentaires sur la configuration et l'utilisation de l'iDRAC au sein de votre système.

- Le **guide des API Redfish de l'iDRAC** fournit des informations sur l'API Redfish.
- Le document Guide de l'interface de ligne de commande RACADM d'Integrated Dell Remote Access Controller fournit des informations sur les sous-commandes RACADM, les interfaces prises en charge, ainsi que les groupes de bases de données de propriétés et les définitions d'objets de l'iDRAC.
- Le *Guide de présentation de la gestion des systèmes* fournit des informations sommaires sur les logiciels disponibles pour exécuter des tâches de gestion des systèmes.
- Le **Guide de l'utilisateur de Dell Remote Access Configuration Tool** explique comment utiliser l'outil de détection des adresses IP de l'iDRAC dans le réseau et comment exécuter des mises à jour de firmware un à plusieurs et des configurations Active Directory pour les adresses IP détectées.
- Le document **Matrice de support 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 de l'utilisateur d'iDRAC Service Module** fournit des informations sur l'installation d'iDRAC Service Module.
- 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 de l'utilisateur des utilitaires de gestion des contrôleurs Dell OpenManage BMC** 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 **Registre d'attributs d'Integrated Dell Remote Access Controller 10** fournit des détails sur les groupes et les objets dans la base de données de propriétés de l'iDRAC.

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

- Les Consignes de sécurité fournies avec votre système contiennent des informations importantes sur la sécurité et réglementaires en vigueur. Pour plus d'informations réglementaires, voir la page d'accueil Conformité aux normes sur le site Web **dell.com/regulatory_compliance**. Les 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 une vue d'ensemble des fonctions du système, de sa configuration, ainsi que de ses caractéristiques techniques.

- Le *Manuel d'installation et de maintenance* présente des informations sur les caractéristiques du système, ainsi que des instructions relatives à son dépannage et à l'installation ou au remplacement de composants système.

Contacter Dell

Dell met à la disposition des clients plusieurs options de support et services en ligne ou par téléphone. La disponibilité varie selon le pays ou la zone géographique et le produit. Il est possible que certains services ne soient pas disponibles dans votre région. Si vous souhaitez contacter Dell pour des questions d'ordre commercial, de support technique ou de service après-vente, rendez-vous sur Contacter Dell.

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

Accès aux documents à partir du site de support Dell

Cliquez sur les liens suivants pour accéder aux documents à partir du site de support Dell :

- Documents sur la gestion des systèmes Enterprise et OpenManage Connections
- Documents sur OpenManage
- Documents sur iDRAC et Lifecycle Controller
- Documents sur les outils de facilité de maintenance
- Documents sur la gestion des systèmes Client Command Suite

Accès aux documents à l'aide de la recherche de produit

1. Rendez-vous sur le site de support Dell.
2. Dans la zone de recherche **Saisissez une étiquette de service**, **un numéro de série...**, saisissez le nom du produit. Par exemple, **PowerEdge** ou **iDRAC**. Une liste de produits correspondants s'affiche.
3. Sélectionnez votre produit et cliquez sur l'icône de recherche ou appuyez sur entrée.
4. Cliquez sur **DOCUMENTATION**.
5. Cliquez sur **MANUELS ET DOCUMENTS**.

Accès aux documents à l'aide de la sélection de produits

Vous pouvez également accéder aux documents en sélectionnant votre produit.

1. Rendez-vous sur le site de support Dell.
2. Cliquez sur **Parcourir tous les produits**.
3. Cliquez sur la catégorie de produit souhaitée : Serveurs, Logiciel, Stockage, etc.
4. Cliquez sur le produit souhaité, puis sur la version le cas échéant.

   REMARQUE : Pour certains produits, vous devrez peut-être parcourir les sous-catégories.

5. Cliquez sur **DOCUMENTATION**.
6. Cliquez sur **MANUELS ET DOCUMENTS**.

Accès à l'API Redfish

Le guide d'accès à l'API Redfish est désormais disponible sur le site Dell API Marketplace.

1. Accédez au portail de développeurs.
2. Cliquez sur **Explorer les API**, puis sur **API**.
3. Sous l'API iDRAC10 Redfish, cliquez sur **Afficher plus**.

2

Ouverture de session dans iDRAC

Vous pouvez vous connecter à iDRAC en tant qu'utilisateur iDRAC, Microsoft Active Directory ou LDAP (Lightweight Directory Access Protocol). Vous pouvez également ouvrir une session à l'aide de OpenID Connect, de la connexion directe ou par carte à puce.

Pour plus de sécurité, chaque système dispose d'un mot de passe unique pour iDRAC, disponible sur son étiquette d'informations. Ce mot de passe unique renforce la sécurité de l'iDRAC et de votre serveur. Le nom d'utilisateur par défaut est **root**.

Quand vous commandez un système, vous pouvez choisir de conserver le mot de passe existant (calvin) comme mot de passe par défaut. Dans ce cas, le mot de passe ne figure pas sur l'étiquette d'informations du système.

Dans cette version, DHCP est activé par défaut et l'adresse IP iDRAC est allouée de manière dynamique.

REMARQUE :

- Vous devez disposer du privilège de connexion au contrôleur iDRAC pour pouvoir ouvrir une session iDRAC.
- L'interface utilisateur de l'iDRAC ne prend pas en charge les boutons de navigateur comme **Reculer**, **Avancer** ou **Actualiser**.
- Après la détection de l'adresse IP de l'iDRAC, la connexion à l'iDRAC peut prendre jusqu'à cinq minutes. Si vous ne parvenez pas à vous connecter, contactez l'équipe de support technique.

Bannière de sécurité personnalisable

Vous pouvez personnaliser les avis de sécurité qui s'affichent sur la page d'ouverture de session. Vous pouvez utiliser SSH, RACADM ou Redfish pour personnaliser l'avis. En fonction de votre langue, l'avis peut se présenter au format UTF-8 à 1 024 ou 512 caractères.

Sujets :

Forcer la modification du mot de passe (FCP)

La fonction « Forcer la modification du mot de passe » vous invite à modifier le mot de passe par défaut de l'appareil. Cette fonctionnalité peut être activée dans le cadre de la configuration d'usine.

L'écran FCP s'affiche une fois l'authentification de l'utilisateur réussie. Elle ne peut pas être ignorée. Une fois que l'utilisateur a saisi un mot de passe, l'accès et le fonctionnement normaux sont autorisés. L'état de cet attribut n'est pas affecté par une opération de redéfinition de la configuration par défaut.

REMARQUE : Pour définir ou réinitialiser l'attribut FCP, vous devez disposer des privilèges de connexion et de configuration utilisateur.

REMARQUE : Lorsque la fonction FCP est activée, le paramètre « Avertissement de mot de passe par défaut » est désactivé après la modification du mot de passe utilisateur par défaut.

REMARQUE : Lorsque l'utilisateur root se connecte via l'authentification par clé publique (PKA), le protocole FCP est contourné.

Lorsque la fonction FCP est activée, les actions suivantes ne sont pas autorisées :

- Se connecter à l'iDRAC via n'importe quelle interface utilisateur qui utilise l'interface de ligne de commande avec les informations d'identification de l'utilisateur par défaut, à l'exception de l'interface IPMIpover-LAN.
- Connectez-vous à l'iDRAC via l'application OMM à l'aide de Quick Sync-2.

Ouverture de session dans iDRAC en tant qu'utilisateur local, utilisateur Active Directory ou utilisateur LDAP

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

Vous pouvez configurer le nom d'utilisateur, le mot de passe et les autorisations d'accès d'un utilisateur iDRAC nouveau ou existant à l'aide de l'option **Ajouter/Modifier l'utilisateur** dans l'interface graphique de l'iDRAC.

Pour configurer l'utilisateur, utilisez un nom d'utilisateur unique. Il doit contenir 16 caractères, espaces compris. Les caractères suivants sont pris en charge :

- 0 à 9
- A-Z
- a-z
- Caractères spéciaux : + %) > $ [| ! & = * . , - {] # (? < ; _ } I ^

Lorsque le nom d'utilisateur est modifié, le nouveau ne s'affichera dans l'interface Web qu'à la prochaine connexion de l'utilisateur.

REMARQUE : N'utilisez pas d'espace avant ou après le nom d'utilisateur.

Le champ Mot de passe peut contenir jusqu'à 127 caractères. Les caractères sont masqués. Les caractères suivants sont pris en charge :

- 0 à 9
- A-Z
- a-z
- Caractères spéciaux : + & ? >-} |. ! (' , _ [" @ #) * ; $] / % = < : { I \ `

REMARQUE : Pour améliorer la sécurité, il est recommandé d'utiliser des mots de passe complexes qui comportent 8 caractères ou plus et d'y inclure des lettres minuscules, majuscules, des chiffres et des caractères spéciaux. Il est également recommandé de changer régulièrement ces mots de passe, si possible.

REMARQUE : Le nom d'utilisateur n'est pas sensible à la casse pour un utilisateur Active Directory. Le mot de passe est sensible à la casse pour tous les utilisateurs.

REMARQUE : Outre Active Directory, les services d'annuaire openLDAP, openDS, Novell eDir et Fedora sont pris en charge

REMARQUE : L'authentification LDAP à l'aide d'OpenDS est prise en charge. La clé DH doit être supérieure à 768 bits.

REMARQUE : La fonctionnalité RSA peut être configurée et activée pour les utilisateurs LDAP, mais RSA ne prend pas en charge les LDAP configurés sur Microsoft Active Directory. Par conséquent, la connexion de l'utilisateur LDAP échoue. RSA est pris en charge uniquement pour OpenLDAP.

Pour ouvrir une session dans l'iDRAC en tant qu'utilisateur local, utilisateur Active Directory ou utilisateur LDAP :

1. Ouvrez un navigateur web pris en charge.
2. Dans le champ **Adresse**, saisissez `https://[iDRAC-IP-address]`, puis appuyez sur Entrée.

REMARQUE : Si le numéro de port HTTPS par défaut (port 443) change, saisissez : `https://[iDRAC-IP-address]:[port-number]` où `[iDRAC-IP-address]` est l'adresse IPv4 ou IPv6 iDRAC et `[port-number]` est le numéro de port HTTPS.

La page **Connexion** apparaît.

3. Pour un utilisateur local :
   - Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez votre nom d'utilisateur et votre mot de passe iDRAC.
   - Dans le menu déroulant **Domaine**, sélectionnez **Cet iDRAC**.
4. Dans le cas d'un utilisateur Active Directory, dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe Active Directory. Si le nom de domaine fait partie du nom d'utilisateur, sélectionnez **Cet iDRAC** dans le menu déroulant. Le format du nom d'utilisateur peut être le suivant : <domaine>\<nom d'utilisateur>, <domaine>/<nom d'utilisateur> ou <utilisateur>@<domaine>.

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

   Le domaine Active Directory du menu déroulant **Domain** affiche le dernier domaine utilisé.
5. Pour un utilisateur LDAP, dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez votre nom d'utilisateur et votre mot de passe LDAP. Le nom de domaine n'est pas requis pour la connexion LDAP. Par défaut, **Cet iDRAC** est sélectionné dans le menu déroulant.
6. Cliquez sur **Envoyer**. Vous êtes connecté à l'iDRAC avec les privilèges d'utilisateur requis.

   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.

Ouverture de session dans l'iDRAC 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 :

- Téléchargez le certificat d'utilisateur de carte à puce et le certificat d'autorité de certification (CA) de confiance vers l'iDRAC.
- Activez l'ouverture de session par carte à puce.

L'interface Web d'iDRAC affiche la page d'ouverture de session par carte à puce pour les utilisateurs configurés utilisent une carte à puce.

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

1. Accédez à l'interface Web de l'iDRAC à l'aide du lien `https://[IP address]`.

   La page **Ouverture de session iDRAC** qui apparaît vous invite à insérer la carte à puce.

   REMARQUE : Si le numéro de port HTTPS par défaut (port 443) change, saisissez : `https://[IP address]:[port number]` où `[IP address]` est l'adresse IP de l'iDRAC et `[port number]` est le numéro de port HTTPS.
2. Insérez la carte à puce dans le lecteur et cliquez sur **Connexion**.
   Une invite demandant le code PIN de la carte à puce s'affiche. Aucun mot de passe n'est requis.
3. Saisissez le code PIN de la carte pour les utilisateurs de carte à puce locaux.

   Vous avez ouvert une session sur l'iDRAC.

   REMARQUE : Si vous êtes un utilisateur local pour lequel l'option **Activer le contrôle CRL pour la connexion par carte à puce** est activée, l'iDRAC tente de télécharger la liste de révocation des certificats (CRL) et vérifie la liste CRL pour le certificat de l'utilisateur. La connexion échoue si le certificat est répertorié comme révoqué dans la liste de révocation des certificats ou si la liste CRL ne peut pas être téléchargée pour une raison quelconque.

   REMARQUE : Si vous vous connectez à l'iDRAC à l'aide d'une carte à puce lorsque RSA est activé, le jeton RSA est contourné et vous pouvez vous connecter directement.

Ouverture de session dans l'iDRAC comme utilisateur Active Directory par carte à puce

Avant de vous connecter en tant qu'utilisateur Active Directory en utilisant une carte à puce, vérifiez les points suivants :

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

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

1. Connectez-vous à l'iDRAC en cliquant sur le lien `https://[IP address]`.

   La page **Ouverture de session iDRAC** qui apparaît vous invite à insérer la carte à puce.

   REMARQUE : Si le numéro de port HTTPS par défaut (port 443) change, saisissez : `https://[IP address]:[port number]`, `[IP address]` représentant l'adresse IP de l'iDRAC et `[port number]` le numéro de port HTTPS.

2. Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.
   Une invite demandant le **code PIN** de la carte à puce s'affiche.
3. Saisissez le code PIN, puis cliquez sur **Envoyer**.

   Vous êtes connecté à l'iDRAC avec vos références 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.

   REMARQUE : Pour les stations de travail client qui font partie du domaine Active Directory, l'utilisation de la carte à puce limite la profondeur de la chaîne de certificats à 10. Cependant, l'utilisation d'une carte à puce sur des stations de travail client hors domaine n'est pas limitée à une profondeur de la chaîne de certificats client.

Ouverture d'une session iDRAC à l'aide de l'authentification unique

Lorsque l'authentification unique (SSO) est activée, vous pouvez ouvrir une session dans iDRAC sans entrer vos références d'utilisateur de domaine, telles que le nom d'utilisateur et le mot de passe.

REMARQUE : Lorsqu'un utilisateur AD configure l'authentification unique (SSO) alors que RSA est activé, le jeton RSA est contourné et l'utilisateur se connecte directement.

Ouverture d'une session dans iDRAC par connexion directe (SSO) à l'aide de l'interface Web iDRAC

Avant de vous connecter à l'iDRAC via l'authentification unique (SSO), vérifiez les points suivants :

- Vous vous êtes connecté au système en utilisant un compte utilisateur Active Directory.
- L'option d'authentification unique est activée pendant la configuration Active Directory.

Pour ouvrir une session dans l'iDRAC à l'aide de l'interface Web :

1. Ouvrez une session sur votre poste de gestion en utilisant un compte Active Directory valide.
2. Dans un navigateur Web, saisissez `https://[FQDN address]`.

   REMARQUE : Si le numéro de port HTTPS par défaut (port 443) a été modifié, saisissez : `https://[FQDN address]:[port number]`, `[FQDN address]` représentant le nom FQDN de l'iDRAC (nom iDRACdnsname.domain.) et `[port number]` 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.

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

Accès à l'iDRAC à l'aide de l'interface distante RACADM

Les interfaces RACADM distante et locale, qui font partie de la CLI RACADM, ne sont pas disponibles dans la version iDRAC10 1.10.17.00. Toutefois, vous pouvez utiliser l'interface de ligne de commande RACADM via l'interface SSH de l'iDRAC.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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

REMARQUE : Le certificat iDRAC est le certificat que l'iDRAC envoie au client RACADM afin d'établir la session sécurisée. Ce certificat est émis par une autorité de certification ou est autosigné. Dans les deux cas, si la station de gestion ne reconnaît pas l'autorité de certification ou l'autorité de signature, un message d'avertissement s'affiche.

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 du format DER au 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 par défaut du bundle de certificats d'autorité de certification sur la station de gestion. Par exemple, l'emplacement de RHEL 64 bits est **/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 `cat command: cat testcacert.pem >> cert.pem`
4. Générez et envoyez le certificat serveur à iDRAC.

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

Les interfaces RACADM distante et locale, qui font partie de la CLI RACADM, ne sont pas disponibles dans la version iDRAC10 1.10.17.00. Toutefois, vous pouvez utiliser l'interface de ligne de commande RACADM via l'interface SSH de l'iDRAC. Pour plus d'informations sur l'accès à l'iDRAC à l'aide de l'interface RACADM locale, voir le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Accès à l'iDRAC à l'aide de RACADM du firmware

Vous pouvez utiliser l'interface SSH pour accéder à l'iDRAC et exécuter les commandes RACADM du firmware. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Authentification simple à deux facteurs (2FA simple)

Pour renforcer la sécurité, l'iDRAC offre une option d'authentification simple à 2 facteurs aux utilisateurs locaux. Lorsque vous vous connectez à partir d'une adresse IP source différente de la dernière connexion, vous êtes invité à saisir les informations d'authentification à deux facteurs.

Quel que soit le moment où vous vous connectez et quel que soit l'intervalle de temps, une seule adresse IP source est mémorisée pour la connexion.

L'authentification simple à deux facteurs comporte deux étapes d'authentification :

- Nom d'utilisateur et mot de passe iDRAC
- Code à 6 chiffres simple envoyé à l'utilisateur par e-mail. L'utilisateur doit saisir ce code à 6 chiffres lorsqu'il y est invité au moment de la connexion.

Le délai d'expiration peut être défini, ce qui permet à un utilisateur 2FA de s'authentifier régulièrement, que l'adresse IP change ou non. L'utilisateur peut définir la plage du délai d'expiration.

REMARQUE :
- Pour recevoir un code à 6 chiffres, il est obligatoire de configurer l'adresse personnalisée de l'expéditeur et de disposer d'une configuration SMTP valide.
- Le code 2FA expire après l'intervalle de temps configuré ou est invalidé s'il est déjà consommé avant l'expiration.
- Si un utilisateur tente de se connecter depuis un autre emplacement avec une adresse IP différente alors qu'une vérification 2FA pour l'adresse IP d'origine est toujours en attente, le même jeton est envoyé pour une tentative de connexion à partir de la nouvelle adresse IP.
- Cette fonctionnalité est disponible avec la licence iDRAC Enterprise ou Datacenter.

Lorsque la fonction 2FA est activée, les actions suivantes ne sont pas autorisées :

- Connectez-vous à l'iDRAC via n'importe quelle interface utilisateur avec les informations d'identification utilisateur par défaut.
- Connectez-vous à l'iDRAC via l'application OMM, via Quick Sync-2

REMARQUE : Les éléments RACADM, Redfish, IPMI LAN, Série, CLI provenant d'une adresse IP source fonctionnent uniquement après connexion aux interfaces prises en charge, comme l'interface utilisateur graphique de l'iDRAC et SSH.

RSA SecurID 2FA

L'iDRAC peut être configuré pour s'authentifier avec un seul serveur RSA AM à la fois. Les paramètres généraux du serveur RSA AM s'appliquent à tous les utilisateurs locaux de l'iDRAC, aux utilisateurs AD et aux utilisateurs LDAP.

REMARQUE : La fonctionnalité RSA SecurID 2FA est disponible uniquement sur la licence Datacenter.

Vous trouverez ci-après les conditions préalables à la configuration de l'iDRAC pour activer RSA SecurID :

- Configurez le serveur Microsoft Active Directory.
- Si vous tentez d'activer RSA SecurID sur tous les utilisateurs AD, ajoutez le serveur AD au serveur RSA AM comme source d'identité.
- Vérifiez que vous disposez d'un serveur LDAP générique.
- Pour tous les LDAP utilisateurs, la source d'identité du serveur LDAP doit être ajoutée au serveur RSA AM.

Pour activer RSA SecurID sur l'iDRAC, les attributs suivants du serveur RSA AM sont requis :

1. **URL de l'API d'authentification RSA** : la syntaxe de l'URL est : `https://<rsa-am-server-hostname>:<port>/mfa/v1_1`, et le port par défaut est 5555.
2. **ID du client RSA** : par défaut, l'ID du client RSA est identique au nom d'hôte du serveur RSA. Localisez l'ID du client RSA sur la page de configuration de l'agent d'authentification du serveur RSA AM.
3. **Clé d'accès RSA** : la clé d'accès peut être récupérée sur RSA AM en accédant à la section **Setup** > **System Settings** > **RSA SecurID** > **Authentication API** qui s'affiche généralement sous la forme `l98cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302`. Pour configurer les paramètres via l'interface graphique de l'iDRAC :
   - Accédez à **Paramètres iDRAC** > **Utilisateurs**.
   - Dans la section **Utilisateurs locaux**, sélectionnez un utilisateur local existant, puis cliquez sur **Modifier**.
   - Défilez vers le bas de la page Configuration.
   - Dans la section **RSA SecurID**, cliquez sur le lien **Configuration de RSA SecurID** pour afficher ou modifier ces paramètres.

   Vous pouvez aussi configurer les paramètres comme suit :
   - Accédez à **Paramètres iDRAC** > **Utilisateurs**.
   - Dans la section **Services d'annuaire**, sélectionnez **Service actif Microsoft** ou **Service d'annuaire LDAP générique**, puis cliquez sur **Modifier**.
   - Dans la section **RSA SecurID**, cliquez sur le lien **Configuration de RSA SecurID** pour afficher ou modifier ces paramètres.
4. **Certificat de serveur RSA AM (chaîne)**

Vous pouvez vous connecter à l'iDRAC à l'aide du jeton RSA SecurID via l'interface graphique de l'iDRAC et SSH.

Application RSA SecurID Token

Vous devez installer l'application RSA SecurID Token sur votre système ou sur un smartphone. Lorsque vous tentez de vous connecter à l'iDRAC, vous êtes invité à saisir le code secret indiqué dans l'application.

Si un code secret incorrect est saisi, le serveur RSA AM demande à l'utilisateur de fournir le « jeton suivant ». Cela peut se produire même si l'utilisateur a saisi le code d'accès correct. Cette saisie prouve que l'utilisateur possède le jeton approprié qui génère le code secret correct.

Pour obtenir le **Jeton suivant** à partir de l'application RSA SecurID Token, cliquez sur **Options**. Cochez **Jeton suivant**. Le code secret suivant est alors disponible. Le délai d'action est essentiel à cette étape. Il est sinon possible que l'iDRAC ne parvienne pas à vérifier le jeton suivant. Si la session de connexion de l'utilisateur de l'iDRAC expire, l'utilisateur doit tenter à nouveau de se connecter.

Si un code secret incorrect est saisi, le serveur RSA AM invite l'utilisateur à fournir le « jeton suivant ». Cette vérification se produit même si l'utilisateur a saisi ultérieurement le mot de passe correct. Cette saisie prouve que l'utilisateur possède le jeton approprié qui génère les codes secrets corrects.

Pour obtenir le jeton suivant à partir de l'application RSA SecurID Token, cliquez sur **Options** et cochez **Jeton suivant**. Un nouveau jeton est généré. Le délai d'action est essentiel à cette étape. Il est sinon possible que l'iDRAC ne parvienne pas à vérifier le jeton suivant. Si la session de connexion utilisateur de l'iDRAC expire, l'utilisateur doit tenter à nouveau de se connecter.

Affichage de l'intégrité du système

Avant d'effectuer une tâche ou de déclencher un événement, vous pouvez utiliser RACADM pour vérifier si le système est dans un état approprié. Pour afficher l'état du service distant à partir de RACADM, utilisez la commande `getremoteservicesstatus`.

REMARQUE : L'état en temps réel s'affiche comme **Non applicable** s'il n'y a pas de contrôleurs compatibles en temps réel sur le système.

Tableau 8. Valeurs possibles pour l'état du système

Système hôte	Lifecycle Controller (LC)	État en temps réel	État général
• Hors tension • Dans POST • Hors POST • Collecte de l'inventaire du système • Exécution de tâches automatisées • Configurateur de serveur unifié Lifecycle Controller • Le serveur s'est arrêté à l'invite d'erreur F1/F2 en raison d'une erreur POST • Le serveur s'est arrêté à l'invite F1/F2/F11, car aucun périphérique amorçable n'est disponible • Le serveur est entré dans le menu de configuration F2 • Le serveur est entré dans le menu de Gestionnaire de démarrage F11	• Prêt • Non initialisé • Rechargement des données • Désactivé • En récupération • En cours d'utilisation	• Prêt • Non prêt • Non applicable	• Prêt • Non prêt

1. Lecture/écriture : lecture seule
2. Privilège utilisateur : utilisateur de connexion
3. Licence requise : iDRAC Core ou iDRAC Enterprise
4. Dépendance : aucune

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

Vous pouvez vous connecter à l'iDRAC via SSH sans saisir 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 comme l'interface distante RACADM, car la session se termine à la fin de la commande.

Par exemple :

Connexion :

```
ssh username@<domain>
```

ou

```
ssh username@<IP_address>
```

où `IP_address` correspond à l'adresse IP de l'iDRAC.

Envoi de commandes RACADM :

```
ssh username@<domain> racadm getversion
```

```
ssh username@<domain> racadm getsel
```

Sessions iDRAC multiples

Le tableau suivant répertorie le nombre de sessions iDRAC possibles à l'aide des diverses interfaces.

Tableau 9. Sessions iDRAC multiples

Interface	Nombre de sessions
Interface web iDRAC	8
Interface RACADM distante	4
firmware RACADM	SSH - 4, série - 1

L'iDRAC autorise plusieurs sessions pour le même utilisateur. Lorsque l'utilisateur a créé le nombre maximal de sessions autorisées, les autres utilisateurs ne peuvent pas se connecter à l'iDRAC. Cela peut entraîner un **déni de service** pour un utilisateur administrateur légitime.

En cas d'épuisement des sessions, appliquez les mesures correctives suivantes :

- Si les sessions basées sur WebServer sont épuisées, vous pouvez toujours vous connecter via l'interface SSH ou RACADM locale.
- Un administrateur peut alors fermer les sessions existantes à l'aide des commandes racadm (`racadm getssninfo` ; `racadm closessn -i <index>`).

Mot de passe sécurisé par défaut

Tous les systèmes pris en charge sont livrés avec un mot de passe par défaut unique pour l'iDRAC, sauf si vous choisissez de définir **calvin** comme mot de passe lorsque vous commandez le système. Ce mot de passe unique renforce la sécurité de l'iDRAC et de votre serveur. Afin de renforcer encore la sécurité, nous vous recommandons de modifier le mot de passe par défaut.

Le mot de passe unique de votre système est indiqué sur l'étiquette d'informations du système. Pour localiser cette étiquette, voir la documentation de votre serveur à l'adresse Page de support Dell.

REMARQUE : La réinitialisation de l'iDRAC aux paramètres d'usine par défaut rétablit le mot de passe par défaut avec lequel le serveur a été livré.

Si vous avez oublié le mot de passe et que vous n'avez pas accès à l'étiquette d'informations système, vous pouvez réinitialiser le mot de passe localement ou à distance en utilisant certaines méthodes.

Rétablissement du mot de passe iDRAC par défaut en local

Si vous avez un accès physique au système, vous pouvez réinitialiser le mot de passe avec ces outils :

- Utilitaire de configuration iDRAC (configuration du système)
- Interface RACADM locale
- OpenManage Mobile
- Port USB de gestion du serveur
- USB-NIC

Rétablissement à distance du mot de passe par défaut de l'iDRAC

Si vous n'avez pas accès au système physiquement, vous pouvez réinitialiser à distance le mot de passe par défaut.

Modification du mot de passe de connexion par défaut

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

- Vous vous connectez à iDRAC avec le privilège de Configuration.
- La fonctionnalité d'avertissement de mot de passe par défaut est activée.
- Par défaut, le nom d'utilisateur et le mot de passe iDRAC sont fournis sur l'étiquette des informations système.

Un message d'avertissement s'affiche également lorsque vous vous connectez à l'iDRAC à l'aide de SSH, de l'interface Web ou de l'interface distante RACADM. Dans le cas de l'interface Web et SSH, un message d'avertissement s'affiche pour chaque session. Pour l'interface distante RACADM, le message d'avertissement s'affiche pour chaque commande.

Modification du mot de passe de connexion par défaut à l'aide de l'interface Web

Lorsque vous ouvrez une session sur l'interface Web iDRAC, 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, procédez comme suit :

1. Sélectionnez l'option **Change Default Password**.
2. Dans le champ **Nouveau mot de passe**, saisissez le nouveau mot de passe.

   REMARQUE : Pour plus d'informations sur les caractères recommandés pour les noms d'utilisateur et les mots de passe, reportez-vous à la section Caractères recommandés dans les noms d'utilisateur et les mots de passe.

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 vous êtes connecté(e) à 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'iDRAC**.

Modification du mot de passe de connexion par défaut à l'aide des commandes RACADM

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

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

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

REMARQUE : L'index du compte par défaut est 2.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

REMARQUE : Pour plus d'informations sur les caractères recommandés pour les noms d'utilisateur et les mots de passe, reportez-vous à la section Caractères recommandés dans les noms d'utilisateur et les mots de passe.

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

Pour modifier le mot de passe de connexion par défaut à l'aide de l'utilitaire de configuration de l'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.

   REMARQUE : Pour plus d'informations sur les caractères recommandés pour les noms d'utilisateur et les mots de passe, reportez-vous à la section Caractères recommandés dans les noms d'utilisateur et les mots 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 de mot de passe par défaut. Pour ce faire, vous devez disposer du privilège Configurer les utilisateurs.

Blocage d'adresse IP

Vous pouvez utiliser le blocage d'adresse IP pour déterminer de manière dynamique si un nombre excessif d'échecs de connexion se produit à partir d'une adresse IP et bloquer ou empêcher l'adresse IP de se connecter à l'iDRAC10 pour une période présélectionnée. Le blocage d'adresse IP inclut :

- Le nombre d'échecs de connexion autorisés.
- Le délai en secondes pendant lequel ces échecs doivent se produire.
- La durée, en secondes, pendant laquelle l'adresse IP n'est pas en mesure d'établir une session après le dépassement du nombre total d'échecs autorisé.

Au fur et à mesure que les échecs de connexion consécutifs s'accumulent à partir d'une adresse IP spécifique, un compteur interne les suit. Quand l'utilisateur parvient à se connecter, l'historique des échecs est effacé et le compteur interne est réinitialisé.

REMARQUE : Lorsque des tentatives de connexion consécutives sont refusées depuis l'adresse IP du client, certains clients SSH peuvent afficher le message suivant :

```
ssh exchange identification: Connection closed by remote host
```

.

REMARQUE : La fonctionnalité de blocage IP prend en charge jusqu'à 5 plages d'adresses IP. Vous pouvez les afficher ou les définir uniquement via RACADM.

Tableau 10. Propriétés de restriction de nouvelles tentatives de connexion

Propriété	Définition
`iDRAC.IPBlocking.BlockEnable`	Active la fonctionnalité de blocage IP. Si des échecs consécutifs `iDRAC.IPBlocking.FailCount` à partir d'une seule adresse IP se produisent dans un laps de temps spécifique `iDRAC.IPBlocking.FailWindow` toutes les tentatives supplémentaires d'établissement d'une session à partir de cette adresse sont rejetées pour une certaine période `iDRAC.IPBlocking.PenaltyTime`
`iDRAC.IPBlocking.FailCount`	Définit le nombre d'échecs de connexion à partir d'une adresse IP avant que les tentatives de connexion ne soient rejetées.
`iDRAC.IPBlocking.FailWindow`	Durée, en secondes, pendant laquelle les tentatives infructueuses sont comptabilisées. Lorsque les échecs se produisent au-delà de ce délai, le compteur est réinitialisé.
`iDRAC.IPBlocking.PenaltyTime`	Définit la période (en secondes) pendant laquelle les tentatives de connexion à partir d'une adresse IP sont rejetées.

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

Pour activer la connexion directe entre le système d'exploitation et l'iDRAC à l'aide de l'interface Web, procédez comme suit :

1. Accédez à **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Connexion directe entre le SE et iDRAC**.
   La page **Connexion directe entre le SE et iDRAC** s'affiche.
2. Modifiez l'état à **Activé**.
3. Sélectionnez l'une des options suivantes pour le mode intermédiaire :
   - **LOM** : le lien de connexion directe du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le périphérique LOM ou OCP.
   - **USB** : le lien de connexion directe du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le bus USB interne.

   REMARQUE : Si vous définissez le mode intermédiaire LOM, assurez-vous que :
   - le système d'exploitation et l'iDRAC se trouvent sur le même sous-réseau ;
   - la sélection de la carte réseau dans les paramètres réseau est définie sur LOM.
4. Si le serveur est connecté en mode LOM partagé, le champ **Adresse IP du SE** est désactivé.

   REMARQUE : Si le VLAN est activé sur l'iDRAC, le transfert LOM ne fonctionne qu'en mode LOM partagé avec le marquage VLAN configuré sur l'hôte.

   REMARQUE :
   - Lorsque le mode de connexion directe est configuré sur LOM, le lancement de l'iDRAC à partir du système d'exploitation hôte après un démarrage à froid est impossible.
   - La connexion directe LOM est supprimée à l'aide de la fonction de mode dédié.
5. Si vous sélectionnez la carte **NIC USB** en tant que configuration de transfert, saisissez l'adresse IP de la carte NIC USB.
   La valeur par défaut est 169.254.1.1. Il est recommandé d'utiliser l'adresse IP par défaut. Toutefois, si cette adresse IP est en conflit avec l'adresse IP des autres interfaces du système hôte ou du réseau local, vous devez la modifier.

Ne saisissez pas les adresses IP 169.254.0.3 et 169.254.0.4. Ces adresses IP sont réservées au port NIC USB du panneau avant lorsqu'un câble USB Type-C est utilisé.

REMARQUE : Si IPv6 est préférable, l'adresse par défaut est fde1:53ba:e9a0:de11::1. Si nécessaire, cette adresse peut être modifiée dans l'iDRAC. Paramètre OS-BMC.UsbNicULA. Si IPv6 n'est pas souhaité sur le USB-NIC, il peut être désactivé en modifiant l'adresse en « :: »

REMARQUE : Lorsque vous modifiez l'adresse IP statique de la carte réseau USB, la plage d'adresses DHCP est automatiquement ajustée pour tenir compte de la nouvelle adresse IP statique. Par exemple, si vous définissez l'adresse IP statique sur 169.254.1.1, l'adresse DHCP est mise à jour sur 169.254.1.2. Cette modification est compatible avec le gestionnaire de réseau Wicked, qui accepte la nouvelle adresse DHCP.

6. Cliquez sur **Appliquer**.
7. 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 des alertes à l'aide de RACADM

Utilisez la commande suivante :

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 — Désactivé

n=1 — Activé

3

Open Server Manager 3.0.x

Vous pouvez effectuer une mise à jour vers Open Server Manager (OSM) 3.0.x à partir de l'iDRAC10.

Sujets :

Préparation du système pour une mise à jour d'OSM

Conditions préalables requises et préparation du système pour une mise à jour d'OSM.

- Vérifiez si OSM est pris en charge sur la plate-forme cible.
- Licence OSM disponible.
- DUP OSM disponible.

1. Vérifiez que les dernières versions d'iDRAC, de FPGA et du BIOS sont en cours d'exécution sur votre système.
2. Téléchargez la licence OSM obtenue auprès de Dell.
3. Assurez-vous qu'OSM est disponible dans l'inventaire du firmware de l'URI Redfish (**redfish/v1/UpdateService/FirmwareInventory**) et l'interface utilisateur de l'iDRAC (**Système** > **Inventaire** > **Inventaire du firmware**).

Mise à jour de d'OSM sur le système

1. Téléchargez le DUP OSM et lancez une mise à jour.
   L'hôte s'éteint automatiquement avant le début de la mise à jour. Si l'hôte ne s'arrête pas, utilisez l'interface disponible (UI, Redfish, IPMI) pour arrêter l'hôte manuellement afin que la mise à jour puisse se poursuivre.
2. À la fin de la mise à jour, l'iDRAC redémarre et démarre avec OSM.
3. Consultez le dernier Guide de l'utilisateur Dell Open Server Manager Built on OpenBMC™ pour connaître les étapes à suivre pour accéder à l'interface utilisateur OSM et à ssh.

4

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

REMARQUE : Pour toute mise à jour nécessitant une réinitialisation/redémarrage de l'iDRAC ou si l'iDRAC est redémarré, il est recommandé de vérifier si l'iDRAC est prêt en attendant quelques secondes, avec un délai d'expiration maximum de 5 minutes, avant d'utiliser une autre commande.

Sujets :

Définition de l'adresse IP d'iDRAC

Vous devez configurer les paramètres réseau initiaux selon l'infrastructure de votre réseau pour activer les communications vers et depuis l'iDRAC. Vous pouvez configurer l'adresse IP à l'aide de l'une des interfaces suivantes :

- Utilitaire de configuration iDRAC
- Lifecycle Controller (voir *Guide de l'utilisateur de Dell Lifecycle Controller*)

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

Après avoir défini l'adresse IP d'iDRAC :

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

Définition de l'adresse IP d'iDRAC à l'aide de l'utilitaire de configuration d'iDRAC

Pour configurer l'adresse IP d'iDRAC :

1. Mettez le système sous tension.
2. Appuyez sur la touche <F2> lors de l'autotest de mise sous tension (POST).
3. Sur la page **System Setup Main Menu** (Menu principal de la configuration du système), 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 :
   - Paramètres réseau
   - Paramètres communs
   - Paramètres IPv4
   - Paramètres IPv6
   - Paramètres IPMI
   - Paramètres VLAN
6. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les informations réseau sont enregistrées et le système redémarre.

Configuration des paramètres du 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 NIC**, sélectionnez **Activé**.
2. Dans la liste **Sélection NIC**, sélectionnez l'un des ports suivants en fonction des exigences réseau :
   - **Dédié** : active le périphérique d'accès distant pour utiliser l'interface réseau disponible sur le contrôleur d'accès à distance (RAC). 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.

     REMARQUE : Cette option implique que le port réseau dédié d'iDRAC achemine son trafic séparément des ports LOM ou NIC du serveur. L'option Dédié permet au contrôleur iDRAC de se voir attribuer une adresse IP du même sous-réseau ou d'un sous-réseau différent par comparaison aux adresses IP affectées au LOM ou aux cartes NIC hôtes pour gérer le trafic réseau.

   - **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.

3. À partir de la **Sélection de NIC** dans le menu déroulant, sélectionnez le port à partir duquel vous souhaitez accéder au système à distance ; voici les options disponibles :

   REMARQUE : Vous pouvez sélectionner la carte d'interface réseau dédiée ou parmi une liste de LOM disponibles dans les cartes mezzanines à quatre ports ou double port.

   - **Pour cartes à quatre ports—LOM1-LOM16**
   - **Pour cartes double port—LOM1, LOM2, LOM5, LOM6, LOM9, LOM10, LOM13, LOM14.**
4. Dans le menu déroulant **Serveur de basculement**, sélectionnez l'un des LOM restants. Si un réseau est défaillant, le trafic est routé via le réseau de basculement.

   Par exemple, pour acheminer le trafic réseau iDRAC vers LOM2 lorsque LOM1 est arrêté, sélectionnez **LOM1** comme **Sélection NIC** et **LOM2** comme **Réseau de basculement**.

REMARQUE : Cette option est désactivée si **Sélection de carte réseau** est défini sur **Dédié**.

REMARQUE : Lors de l'utilisation des paramètres du **réseau de basculement**, il est recommandé que tous les ports LOM soient connectés au même réseau.

Pour plus d'informations, reportez-vous à la section modification des paramètres réseau à l'aide de l'interface Web.

5. Sous **Négociation automatique**, sélectionnez **Activé** si iDRAC doit définir automatiquement le mode duplex et la vitesse du réseau. Cette option est disponible uniquement pour le mode dédié. Si elle est activée, iDRAC définit la vitesse de réseau sur 10, 100 ou 1 000 Mbits/s en fonction de la vitesse du réseau.
6. Sous **Réseau Vitesse**, sélectionnez 10 Mbits/s ou 100 Mbits/s.

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

   REMARQUE : Cette option est désactivée si **Négociation automatique** est définie sur **Activée**.

   REMARQUE : Si l'équipe réseau est configuré pour le système d'exploitation de l'hôte à l'aide de la même carte réseau que sous Sélection de NIC, alors le réseau de basculement doit également être configuré. La Sélection de NIC et le réseau de basculement doivent utiliser les ports qui sont configurés en tant que partie intégrante de l'équipe réseau. Si plus de deux ports sont utilisés dans le cadre de l'équipe réseau, alors la sélection du réseau de basculement doit être « Tous ».
8. Sous **MTU NIC**, saisissez la taille de l'unité de transmission maximale (MTU) de la carte réseau (NIC).

   REMARQUE : La limite maximale par défaut pour la MTU sur une carte NIC est de 1 500 et la valeur minimale est de 576. Une valeur MTU de 1280 ou plus est requise si le protocole IPv6 est activé.

Paramètres communs

Si l'infrastructure réseau possède un serveur DNS, enregistrez l'iDRAC sur le DNS. Il s'agit des paramètres initiaux requis pour les fonctionnalités avancées, telles que les services d'annuaire : Active Directory ou LDAP, authentification unique (SSO) et carte à puce.

Pour enregistrer iDRAC :

1. Sélectionnez **Enregistrer le DRAC auprès du DNS**
2. Saisissez le **nom DNS DRAC**.
3. Sélectionnez **Configuration automatique du nom de domaine** pour acquérir automatiquement un nom de domaine à partir de DHCP. Sinon, fournissez le **Nom de domaine DNS**.

   Pour le champ **Nom de l'iDRAC DNS**, le format de nom par défaut est **idrac-Service_Tag**, Service_Tag étant l'étiquette de service du serveur. La longueur maximale est de 63 caractères et les caractères suivants sont pris en charge :
   - A-Z
   - a-z
   - 0 à 9
   - Tiret (-)

Configuration des paramètres IPv4

Pour configurer les paramètres Ipv4, procédez comme suit :

1. Sélectionnez l'option **Activé** sous **Activer IPv4**.
2. Sélectionnez l'option **Activé** sous **Activer DHCP** afin que le DHCP puisse automatiquement attribuer l'adresse IP, la passerelle et le masque de sous-réseau à l'iDRAC. Vous pouvez aussi sélectionner **Désactivé** et saisir les valeurs pour :
   - Adresse IP statique
   - Passerelle statique
   - Masque de sous-réseau statique

   Les options **Utiliser DHCP pour obtenir des adresses de serveur DNS**, **Utiliser DHCPv6 pour obtenir des adresses de serveur DNS** et **Configuration automatique du nom de domaine** sont activées par défaut.

Configuration des paramètres IPv6

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

Pour configurer les paramètres iPv6 :

REMARQUE : Si IPv6 est défini sur « statique », assurez-vous de configurer manuellement la passerelle IPv6 (cette étape n'est pas nécessaire pour une adresse IPV6 dynamique). Si vous ne configurez pas manuellement l'adresse IPv6 statique, vous perdrez la communication.

1. Sélectionnez l'option **Activé** sous **Activer IPv6**.
2. Pour que le serveur DHCPv6 affecte automatiquement l'adresse IP et la longueur du préfixe à l'iDRAC, sélectionnez l'option **Activé** sous **Enable Auto-configuration**.

   REMARQUE : Vous pouvez configurer les adresses IP statiques et IP DHCP en même temps.

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 1 et 128.
5. Dans la zone **Passerelle statique**, entrez l'adresse de la passerelle.

   REMARQUE : Si vous configurez une adresse IP statique, l'adresse IP actuelle 1 affiche l'adresse IP statique et l'adresse IP 2 affiche l'adresse IP dynamique. Si vous effacez les paramètres d'adresse IP statique, l'adresse IP actuelle 1 affiche l'adresse IP dynamique.

   Les options **Utiliser DHCP pour obtenir des adresses de serveur DNS**, **Utiliser DHCPv6 pour obtenir des adresses de serveur DNS** et **Configuration automatique du nom de domaine** sont activées par défaut.
6. Effectuez les configurations suivantes, si nécessaire :
   - 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.
7. Lorsque les informations DNS ne sont pas accessibles par la configuration DHCPv6 ou la configuration statique, vous pouvez utiliser RFC 8106 « Options d'annonces du routeur IPv6 pour la configuration DNS ». Il est identifié par le routeur IPv6. L'utilisation de la configuration DNS RA n'a pas d'impact sur les configurations DNS existantes (DHCPv6 ou statique).
   - L'iDRAC peut obtenir des informations sur le serveur de noms DNS et le domaine de recherche DNS à partir des messages d'annonce du routeur IPv6. Reportez-vous au RFC 8106 et au guide de l'utilisateur de votre routeur IPv6 pour plus d'informations sur la façon de configurer le routeur pour annoncer ces informations.
   - Si les informations DNS sont disponibles à partir du serveur DHCPv6 et de l'annonce du routeur IPv6, l'iDRAC utilise les deux. En cas de conflit, les informations DNS du serveur DHCPv6 prévalent dans les paramètres /etc/resolv.conf de l'iDRAC.

   REMARQUE : L'IDRAC utilise les informations DNS RA, IPv6. IPv6.Autoconfig doit être activé. Si la configuration automatique est désactivée, l'iDRAC ne traite pas les messages RA IPv6 et utilise uniquement les paramètres DNS statiques tels qu'ils sont configurés.

Configuration des 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 **Clé de chiffrement**, entrez la clé de chiffrement en utilisant entre 0 et 40 caractères hexadécimaux (sans espaces). La valeur par défaut comporte uniquement des zéros.

Paramètres VLAN

Vous pouvez configurer l'iDRAC dans l'infrastructure VLAN. Pour configurer les paramètres VLAN, effectuez les opérations suivantes :

1. Sous **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.

REMARQUE : Après l'activation de VLAN, l'IP de l'iDRAC n'est pas accessible pendant un certain temps.

Contrôle d'accès au réseau basé sur les ports (IEEE 802.1x)

iDRAC fournit un contrôle d'accès au réseau basé sur les ports (IEEE802.1x). Il offre un mécanisme d'authentification sécurisé aux appareils souhaitant se connecter à un LAN.

Cette fonctionnalité nécessite une licence iDRAC Datacenter.

Cette fonctionnalité est accessible via l'interface graphique de l'iDRAC en vous rendant dans **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Paramètres réseau avancés** > **Sécurité 802.1x**. Vous pouvez activer ou désactiver l'option à l'aide de la liste déroulante. La fonctionnalité est activée par défaut.

REMARQUE : L'effet de la sécurité 802.1x ne fonctionne pas lorsque l'iDRAC est en mode LOM partagé avec le VLAN activé.

Le contrôle d'accès au réseau basé sur les ports offre trois méthodes de configuration des certificats d'authentification :

- **IDevID par défaut** : il s'agit du certificat iDRAC par défaut installé en usine.
- **LDevID de signature personnalisé** : cette option permet de définir une requête de signature de certificat (CSR), laquelle est signée par le certificat de signature LDEVID téléchargé.
- **LDevID personnalisé** : cette option permet de télécharger un certificat personnalisé de votre choix.

Il existe une option permettant d'activer ou de désactiver le **Certificat du serveur d'authentification** dans le but de fournir les informations nécessaires à la validation du certificat. Elle est désactivée par défaut.

REMARQUE :

- Cette fonctionnalité est désactivée par défaut dans les serveurs modulaires.
- Toute modification apportée à la configuration 802.1x, y compris les téléchargements de certificats et l'activation/désactivation de paramètres, prend effet au démarrage suivant de l'iDRAC.
- La commutation réseau de l'iDRAC d'un commutateur activé pour une sécurité 802.1x vers un commutateur activé pour une autre sécurité nécessite un redémarrage de l'iDRAC.
- Si les ports du commutateur Ethernet qui sont connectés aux ports LOM du serveur sont activés pour une sécurité 802.1x, tous les périphériques en aval sur ces ports doivent être activés pour une sécurité 8021.x. Cela signifie que l'hôte est affecté s'il n'a pas été activé pour une sécurité 802.1x.

Détection automatique

La fonctionnalité Détection automatique permet aux serveurs nouvellement installés de détecter automatiquement la console de gestion à distance qui héberge le serveur de provisionnement. Le **serveur de positionnement** fournit à iDRAC les informations d'identification d'administration personnalisées de l'utilisateur pour que le serveur non provisionné puisse être détecté et géré depuis la console de gestion.

La détection automatique fonctionne avec une adresse IP statique. La fonctionnalité de détection automatique sur l'iDRAC est utilisée pour trouver le serveur de provisionnement à l'aide de DHCP/monodiffusion DNS/mDNS.

- Lorsque l'iDRAC possède l'adresse de la console, il envoie sa propre étiquette de service, son adresse IP, son numéro de port Redfish, son certificat Web, etc.
- Ces informations sont publiées régulièrement sur les consoles.

DHCP, le serveur DNS ou le nom de l'hôte DNS par défaut découvre le serveur de provisionnement. Si le DNS est spécifié, l'adresse IP du serveur de provisionnement est extraite du DNS et les paramètres DHCP ne sont pas nécessaires. Si la détection automatique est spécifiée, la détection est ignorée et ni DHCP ni DNS ne sont nécessaires.

La détection automatique peut être activée de l'une des manières suivantes :

1. À l'aide de l'interface utilisateur de l'iDRAC : **Paramètres de l'iDRAC** > **Connectivité** > **Détection automatique de l'iDRAC**
2. Utilisation de l'interface RACADM :`racadm set iDRAC.AutoDiscovery.EnableIPChangeAnnounce 1`

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

1. Mettez le système sous tension.
2. Pendant le POST, appuyez sur F2 et accédez à **Paramètres iDRAC** > **Activation à distance**.
   La page **Activation à distance des paramètres iDRAC** s'affiche.
3. Activez la détection automatique, saisissez l'adresse IP du serveur de provisionnement et cliquez sur **Retour**.

REMARQUE : La définition de l'adresse IP du serveur de provisionnement est facultative. Si vous ne définissez pas cette adresse, elle est découverte en utilisant les paramètres DHCP ou DNS (étape 7).

4. Cliquez sur **Réseau**.
   La page **Paramètres réseau iDRAC** s'affiche.
5. Activez NIC.
6. Activer IPv4

   REMARQUE : IPv6 n'est pas pris en charge pour la détection 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 de provisionnement (étape 3) est fournie.

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

La fonction de configuration automatique configure et met à disposition tous les composants d'un serveur en une seule opération. Ces composants comprennent le BIOS, iDRAC et PERC. La configuration automatique importe automatiquement un fichier JSON ou XML de profil de configuration de serveur (SCP) contenant tous les paramètres configurables. Le serveur DHCP qui attribue l'adresse IP contient également les détails d'accès au fichier SCP.

Les fichiers SCP sont créés par la configuration d'un serveur de configuration Or. Cette configuration est alors exportée vers un emplacement réseau partagé NFS, CIFS, HTTP ou HTTPS qui est accessible par le serveur DHCP et iDRAC du serveur en cours de configuration. Le nom du fichier SCP peut être basé sur l'étiquette de service ou le numéro de modèle du serveur cible. Il peut aussi avoir un nom générique. Le serveur DHCP utilise une option de serveur DHCP pour spécifier le nom du fichier SCP (éventuellement), l'emplacement du fichier SCP et les informations d'identification permettant d'accéder à l'emplacement du fichier.

Lorsque l'iDRAC obtient une adresse IP auprès du serveur DHCP qui est configuré pour une configuration automatique, iDRAC utilise le SCP pour configurer les périphériques du serveur. La configuration automatique est appelée uniquement après que l'iDRAC obtient son adresse IP du serveur DHCP. S'il n'obtient pas de réponse ou d'adresse IP du serveur DHCP, la configuration automatique DHCP n'est pas appelée.

Les options de partage de fichiers HTTP et HTTPS sont prises en charge pour l'iDRAC. Les détails de l'adresse HTTP ou HTTPS doivent être fournis. Au cas où le proxy serait activé sur le serveur, l'utilisateur doit fournir d'autres paramètres de proxy pour permettre à HTTP ou HTTPS de transférer des informations. La balise d'option `-s` est mis à jour comme suit :

Tableau 11. Différents types de partage et valeurs de transfert

-s (ShareType)	transfert
NFS	`0` ou `nfs`
CIFS	`2` ou `cifs`
HTTP	`5` ou `http`
HTTPS	`6` ou `https`

REMARQUE : Les certificats HTTPS ne sont pas pris en charge avec la configuration automatique. La configuration automatique ignore les avertissements de certificat.

La liste suivante décrit les paramètres requis et facultatifs à transférer pour la valeur de chaîne :

`-f (Filename)` : nom du fichier de profil de configuration de serveur exporté.

`-n (Sharename)` : nom du partage réseau. Ceci est requis pour NFS ou CIFS.

`-s (ShareType)` : transférez 0 pour NFS, 2 pour CIFS, 5 pour HTTP et 6 pour HTTPS.

`-i (IPAddress)` : adresse IP du dossier de partage réseau. Il s'agit d'un champ obligatoire.

`-u (Username)` : nom d'utilisateur qui permet d'accéder au partage réseau. Ce champ est obligatoire pour CIFS.

`-p (Password)` : mot de passe utilisateur qui permet d'accéder au partage réseau. Ce champ est obligatoire pour CIFS.

`-d (ShutdownType)` : 0 pour normal ou 1 pour forcé (paramètre par défaut : 0). Ce champ est facultatif.

`-t (Timetowait)` : temps d'attente qui s'écoule avant l'arrêt de l'hôte (paramètre par défaut : 300). Ce champ est facultatif.

`-e (EndHostPowerState)` : 0 pour DÉSACTIVÉ ou 1 pour ACTIVÉ (paramètre par défaut : 1). Ce champ est facultatif.

Les indicateurs d'option supplémentaires sont pris en charge pour activer la configuration des paramètres de proxy HTTP et définir le délai d'expiration de nouvelle tentative pour l'accès au fichier de profil :

`—pd (ProxyDefault)` : utiliser le paramètre de proxy par défaut. Ce champ est facultatif.

`—pt (ProxyType)` : l'utilisateur peut transférer `http` ou `socks` (paramètre par défaut : http). Ce champ est facultatif.

`—ph (ProxyHost)` : adresse IP de l'hôte proxy. Ce champ est facultatif.

`—pu (ProxyUserName)` : nom d'utilisateur permettant d'accéder au serveur proxy. Ceci est requis pour la prise en charge d'un serveur proxy.

`—pp (ProxyPassword)` : mot de passe utilisateur permettant d'accéder au serveur proxy. Ceci est requis pour la prise en charge d'un serveur proxy.

`—po (ProxyPort)` : port du serveur proxy (le paramètre par défaut est 80). Ce champ est facultatif.

`—to (Timeout)` : indique le délai d'expiration de nouvelle tentative en minutes pour l'obtention du fichier config (la valeur par défaut est 60 minutes).

Les fichiers de profil au format JSON sont pris en charge. Les noms de fichier suivants sont utilisés si le paramètre de nom de fichier n'est pas présent :

- <étiquette de service>-config.xml. Exemple : CDVH7R1-config.xml
- <numéro de modèle> -config.xml. Exemple : R640-config.xml
- config.xml
- <étiquette de service>-config.json. Exemple : CDVH7R1-config.json
- <numéro de modèle>-config.json. Exemple : R630-config.json
- config.json

REMARQUE :

- La configuration automatique peut être activée uniquement lorsque les options **DHCPv4** et **Activer IPV4** sont activées.
- Les fonctions de configuration automatique et de découverte automatique sont mutuellement exclusives. Désactivez la découverte automatique pour que la configuration automatique puisse fonctionner.
- La configuration automatique se désactive dès qu'un serveur effectue une opération de configuration automatique.

Si tous les serveurs Dell PowerEdge du pool de serveurs DHCP sont du même type et portent le même numéro de modèle, un seul fichier SCP (`config.xml`) est obligatoire. Le nom de fichier (`config.xml`) est utilisé en tant que nom de fichier SCP par défaut. Outre le fichier `.xml`, les fichiers `.json` peuvent également être utilisés avec les systèmes 15/16G. Le fichier peut être `config.json`.

L'utilisateur peut configurer des serveurs individuels nécessitant différents fichiers de configuration adressés à l'aide des numéros de service de serveurs individuels ou de modèles de serveur. Dans un environnement disposant de serveurs différents avec des exigences spécifiques, vous pouvez utiliser différents noms de fichier SCP pour distinguer chaque serveur ou type de serveur.

REMARQUE : L'agent de configuration de serveur de l'iDRAC génère automatiquement le nom de fichier de configuration à l'aide de l'étiquette de service du serveur, du numéro de modèle ou du nom de fichier par défaut, `config.xml`.

REMARQUE : Si aucun de ces fichiers ne se trouve sur le partage réseau, la tâche d'importation de profil de configuration de serveur est marquée comme étant en échec en raison du fichier introuvable.

Séquence de configuration automatique

1. Créer ou modifier le fichier SCP qui configure les attributs de serveurs Dell.
2. Placer le fichier SCP 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 SCP dans le champ de l'option fournisseurs 43 du serveur DHCP.
4. Lors de l'acquisition de l'adresse IP, l'iDRAC annonce l'identifiant de la classe de fournisseur. (Option 60)
5. Le serveur DHCP met en correspondance la classe de fournisseur avec l'option de fournisseur dans le fichier `dhcpd.conf` et envoie l'emplacement du fichier SCP et, s'il est indiqué, le nom du fichier SCP à l'iDRAC.
6. L'iDRAC traite le fichier SCP et configure tous les attributs répertoriés dans le fichier.

Options DHCP

DHCPv4 permet de transmettre de nombreux paramètres définis globalement aux clients DHCP. Chaque paramètre est appelé option DHCP. Chaque option est identifiée par une balise d'option, qui correspond à une valeur de 1 octet. Les balises d'option 0 et 255 sont réservées respectivement au remplissage et à la fin des options. Toutes les autres valeurs sont disponibles pour définir les options.

L'option DHCP 43 est utilisée pour envoyer des informations du serveur DHCP au client DHCP. L'option est définie sous la forme d'une chaîne de texte. Cette chaîne de texte contient les valeurs du nom de fichier SCP, l'emplacement du partage et les informations d'identification permettant d'accéder à cet emplacement. Par exemple :

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.255.0 {
# 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 vendor-class-identifier "iDRAC";
    set vendor-string = option vendor-class-identifier;
    option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d 0
-t 500";
```

où, -i est l'emplacement du partage de fichiers à distance et -f est le nom de fichier dans la chaîne avec les informations d'identification pour le partage de fichiers à distance.

L'option DHCP 60 identifie et associe un client DHCP à un fournisseur particulier. Les options 60 et 43 doivent être définies sur tout serveur DHCP configuré pour prendre des mesures en fonction de l'ID fournisseur d'un client. Sur les serveurs Dell PowerEdge, l'iDRAC s'identifie avec l'ID de fournisseur : **iDRAC**. Par conséquent, vous devez ajouter une nouvelle « classe de fournisseurs » et créer une « option de périmètre » sous celle-ci pour le « code 60 », puis activer la nouvelle option de périmètre pour le serveur DHCP.

Configuration de l'option 43 sur Windows

Pour configurer l'option 43 sur Windows :

1. Sur le serveur DHCP, accédez à **Démarrer** > **Outils d'administration** > **DHCP** pour ouvrir l'outil d'administration du 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 saisissez l'adresse IP du serveur sur lequel se situe l'emplacement de partage, qui contient le fichier SCP.
   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, accédez à **Démarrer** > **Outils d'administration** > **DHCP** pour ouvrir l'outil d'administration du 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 **Ajouter**.
   Une boîte de dialogue comportant les champs suivants s'affiche :
   - **Nom d'affichage :**
   - **Description :**
   - **ID : binaire : ASCII :**
5. Dans le champ **Nom d'affichage :**, entrez `iDRAC` .
6. Dans le champ **Description :**, entrez `Classe de fournisseur`.
7. Cliquez dans la section **ASCII :** et entrez `iDRAC`.
8. Cliquez sur **OK**, puis sur **Fermer**.
9. Dans la fenêtre DHCP, cliquez avec le bouton droit sur **IPv4**, puis sélectionnez **Configurer les options prédéfinies**.

10. Dans le menu déroulant **Classe d'options**, sélectionnez **iDRAC** (créé à l'étape 4), puis cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Type d'option**, saisissez les informations suivantes :
    - **Nom** : `iDRAC`
    - **Type de données** : chaîne
    - **Code** : 060
    - **Description** : identifiant de classe de fournisseur Dell
12. Cliquez sur **OK** pour revenir à la fenêtre **DHCP**.
13. Développez tous les éléments situés sous le nom du serveur, effectuez un clic droit sur **Options d'étendue**, puis sélectionnez **Configurer les options**.
14. Cliquez sur l'onglet **Avancé**.
15. Dans la liste **Classe de fournisseur**, sélectionnez **iDRAC**.
    L'`iDRAC 060` s'affiche dans la colonne **Options disponibles**.
16. Sélectionnez l'option **060 iDRAC**.
17. Saisissez la valeur de chaîne qui doit être envoyée à l'iDRAC (ainsi qu'une adresse IP standard de DHCP). La valeur de chaîne facilite l'importation du fichier SCP 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 (-f)` : indique le nom du fichier du profil de configuration de serveur (SCP) exporté.
    - `Sharename (-n)` : indique le nom du partage réseau.
    - `ShareType (-s)` : outre la prise en charge du partage de fichiers NFS et CIFS, le firmware iDRAC assure également la gestion de l'accès aux fichiers de profil à l'aide des protocoles HTTP et HTTPS. La balise `-s option` est mise à jour comme suit : `-s (ShareType):` saisissez nfs ou 0 pour NFS ; cifs ou 2 pour CIFS ; http ou 5 pour HTTP ; ou https ou 6 pour HTTPS (obligatoire).
    - `IPAddress (-i)` : indique l'adresse IP du partage de fichiers.

      REMARQUE : `Sharename (-n)`, `ShareType (-s)` et `IPAddress (-i)` sont des attributs obligatoires qui doivent être transmis. -n n'est pas requis pour HTTP ou HTTPS.
    - `Username (-u)` : indique le nom d'utilisateur requis pour accéder au partage réseau. Cette information est requise uniquement pour CIFS.
    - `Password (-p)` : indique le mot de passe requis pour accéder au partage réseau. Cette information est requise uniquement pour CIFS.
    - `ShutdownType (-d)` : indique le mode d'arrêt. 0 Indique un arrêt ordinaire et 1 indique un arrêt forcé.

      REMARQUE : Le paramètre par défaut est 0.
    - `Timetowait (-t)` : indique la période d'attente pour le système hôte avant sa mise sous tension. Le paramètre par défaut est 300.
    - `EndHostPowerState (-e)` : indique l'état d'alimentation de l'hôte. 0 Indique HORS TENSION et 1 indique SOUS TENSION. Le paramètre par défaut est 1.

      REMARQUE : `ShutdownType (-d)`, `Timetowait (-t)` et `EndHostPowerState (-e)` sont des attributs facultatifs.

NFS : -f system_config.xml -i 192.168.1.101 et -n /nfs_share -s 0 -d 1
CIFS : -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u <**USERNAME**> -p <**PASSWORD**> -d 1 -t 400
HTTP : -f system_config.json -i 192.168.1.101 -s 5
HTTP : -f http_share/system_config.xml -i 192.168.1.101 -s http
HTTP : -f system_config.xml -i 192.168.1.101 -s http -n http_share
HTTPS : -f system_config.json -i 192.168.1.101 -s https

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

Mettez à jour le fichier `/etc/dhcpd.conf`. Les étapes de configuration des options sont similaires aux étapes réservées à Windows :

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.

```
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 vendor-class-identifier "iDRAC";
  set vendor-string = option vendor-class-identifier;
  option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d 0 -t 500";
    range dynamic-bootp 192.168.0.128 192.168.0.254;
    default-lease-time 21600;
    max-lease-time 43200;
        }
}
```

Les éléments suivants sont les paramètres requis et facultatifs qui doivent être passés dans la chaîne d'identifiant de classe de fournisseur :

- Fichier (-f) : indique le nom du fichier Server Configuration Profile exporté.

  REMARQUE : Pour plus d'informations sur les règles de dénomination des fichiers, reportez-vous à la section Configuration des serveurs et des composants de serveur à l'aide de la configuration automatique.

- Sharename (-n) : indique le nom du partage réseau.
- ShareType (-s) : indique le type de partage. 0 correspond à NFS, 2 à CIFS, 5 à HTTP et 6 à HTTPS.

  REMARQUE : Exemple pour le partage réseau Linux NFS, CIFS, HTTP, HTTPS :
  - **NFS** : `-f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500`

    REMARQUE : Assurez-vous d'utiliser NFS2 ou NFS3 pour le partage réseau NFS.
  - **CIFS** : `-f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400`
  - **HTTP** : `-f system_config.xml -i 192.168.1.101 -s http -n http_share`
  - **HTTPS** : `-f system_config.json -i 192.168.1.101 -s https`

- IPAddress (-i) : indique l'adresse IP du partage de fichiers.

  REMARQUE : Sharename (-n), ShareType (-s) et IPAddress (-i) sont des attributs requis qui doivent être transmis. -n n'est pas requis pour HTTP ou HTTPS.

- Username (-u) : indique le nom d'utilisateur requis pour accéder au partage réseau. Cette information est requise uniquement pour CIFS.
- Password (-p) : indique le mot de passe requis pour accéder au partage réseau. Cette information est requise uniquement pour CIFS.
- ShutdownType (-d) : indique le mode d'arrêt. 0 Indique un arrêt ordinaire et 1 indique un arrêt forcé.

  REMARQUE : Le paramètre par défaut est 0.

- Timetowait (-t) : indique la période d'attente pour le système hôte avant sa mise sous tension. Le paramètre par défaut est 300.
- EndHostPowerState (-e) : indique l'état de l'alimentation de l'hôte. 0 Indique HORS TENSION et 1 indique SOUS TENSION. Le paramètre par défaut est 1.

  REMARQUE : ShutdownType (-d), Timetowait (-t) et EndHostPowerState (-e), sont des attributs facultatifs.

Ce qui suit est un exemple de réservation DHCP statique à partir d'un fichier dhcpd.conf :

```
host my_host {
host my_host {
hardware ethernet b8:2a:72:fb:e6:56;
fixed-address 192.168.0.211;
option host-name "my_host";
option myname " -f r630_raid.xml -i 192.168.0.1 -n /nfs -s 0 -d 0 -t 300";
}
```

REMARQUE : Après avoir modifié le fichier `dhcpd.conf`, assurez-vous de redémarrer le service dhcpd afin d'appliquer les modifications.

Configuration requise avant l'activation de la configuration automatique

Avant d'activer la fonctionnalité Configuration automatique, assurez-vous que les éléments suivants sont déjà définis :

- Le partage réseau pris en charge (NFS, CIFS, HTTP et HTTPS) est disponible sur le même sous-réseau que l'iDRAC et le serveur DHCP. Testez le partage réseau pour vous assurer qu'il est accessible et que le pare-feu et les autorisations utilisateur sont correctement définis.
- Le profil de configuration de serveur est exporté vers le partage réseau. En outre, assurez-vous que les modifications nécessaires du fichier SCP sont terminées, de sorte à appliquer les paramètres corrects après le lancement du processus de configuration automatique.
- Le serveur DHCP est configuré et la configuration DHCP a été mise à jour selon la configuration requise pour que l'iDRAC appelle le serveur et lance la fonction de Configuration automatique.

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'iDRAC, accédez à **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Configuration automatique**. La page **Réseau** s'affiche.
2. Dans la section **Configuration automatique** , sélectionnez l'une des options suivantes dans le menu déroulant **Activer le provisionnement DHCP** :
   - **Activer une fois** : la configuration du composant ne s'effectue qu'une seule fois à l'aide du fichier SCP référencé par le serveur DHCP. La configuration automatique est ensuite désactivée.
   - **Activer une fois après la réinitialisation** : après la réinitialisation de l'iDRAC, la configuration du composant ne s'effectue qu'une seule fois à l'aide du fichier SCP référencé par le serveur DHCP. La configuration automatique est ensuite désactivée.
   - **Désactiver** : désactive la fonction de Configuration automatique.
3. Cliquez sur **Appliquer** pour appliquer le paramètre. La page réseau s'actualise automatiquement.

Activation de la configuration automatique à l'aide de RACADM

Pour activer la fonction de configuration automatique à l'aide de RACADM, utilisez l'objet `iDRAC.NIC.AutoConfig`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Pour plus d'informations sur la fonction Configuration automatique, voir le livre blanc **Zero-Touch, bare-metal server provisioning using the Dell iDRAC with Lifecycle Controller Auto Config feature** disponible à l'adresse Page de support Dell.

Utilisation des mots de passe cryptés pour une sécurité optimisée

Vous pouvez définir des mots de passe utilisateur et des mots de passe BIOS à l'aide d'un format de hachage unidirectionnel. Le mécanisme d'authentification de l'utilisateur n'est pas affecté (excepté pour les protocoles SNMPv3 et IPMI) et vous pouvez indiquer le mot de passe au format texte brut.

Avec la nouvelle fonction de cryptage de mot de passe :

- Vous pouvez générer vos propres hachages SHA256 pour définir les mots de passe utilisateur et BIOS d'iDRAC. Cela vous permet d'inclure les valeurs SHA256 dans le profil de configuration du serveur. Lorsque vous fournissez des valeurs de mot de passe SHA256, vous ne pouvez pas vous authentifier au moyen des protocoles SNMPv3 et IPMI.

REMARQUE : L'interface distante RACADM ou Redfish ne peuvent pas être utilisés pour la configuration/le remplacement du mot de passe crypté pour IDRAC. Vous pouvez utiliser la commande SCP pour la configuration/le remplacement du mot de passe crypté sur l'interface distante RACADM ou Redfish.

- Vous pouvez configurer un modèle de serveur contenant tous les comptes utilisateur iDRAC et les mots de passe BIOS en utilisant le mécanisme de texte brut actuel. Une fois le serveur configuré, vous pouvez exporter son profil de configuration de serveur avec les valeurs de hachage de mot de passe. L'exportation inclut les valeurs de hachage requises pour l'authentification SNMPv3 et IPMI. Après l'importation de ce profil, vous devez utiliser la dernière version de l'outil Dell IPMI. Si vous utilisez une version antérieure, l'authentification IPMI échouera pour les utilisateurs dont le mot de passe est défini avec des valeurs hachées.
- Les autres interfaces comme l'interface graphique de l'iDRAC montreront que les comptes utilisateur sont activés.

Vous pouvez générer le mot de passe crypté avec et sans valeur aléatoire à l'aide de SHA256.

Vous devez disposer des privilèges de contrôle du serveur pour inclure et exporter les mots de passe cryptés.

Si l'accès à tous les comptes est perdu, exécutez l'utilitaire de configuration d'iDRAC ou l'interface RACADM locale et effectuez la tâche de Restauration des valeurs par défaut d'iDRAC.

Si le mot de passe du compte d'utilisateur du contrôleur iDRAC est défini avec le mot de passe crypté SHA256 et non avec d'autres valeurs cryptées (SHA1v3Key, MD5v3Key ou IPMIKey), l'authentification par l'intermédiaire de SNMP v3 et IPMI n'est pas disponible.

Chiffrer un mot de passe à l'aide de RACADM

Pour définir des mots de passe de hachage, utilisez les objets suivants avec la commande `set` :

- iDRAC.Users.SHA256Password
- **iDRAC.Users.SHA256PasswordSalt

REMARQUE : Les champs `SHA256Password` et `SHA256PasswordSalt` sont réservés à l'importation XML et ne sont pas définis à l'aide des outils de ligne de commande. La définition de l'un des champs peut potentiellement empêcher l'utilisateur actuel de se connecter à l'iDRAC. Lors de l'importation d'un mot de passe à l'aide de `SHA256Password`, l'iDRAC ne force pas la vérification de la longueur du mot de passe.

Utilisez la commande suivante pour inclure le mot de passe crypté dans le profil de configuration de serveur exporté :

```
racadm get -f <file name> -l <NFS / CIFS / HTTP / HTTPS share> -u <username> -p <password>
-t <filetype> --includePH
```

Vous devez définir l'attribut Salt lorsque le mot de passe crypté est défini.

REMARQUE : Les attributs ne s'appliquent pas au fichier de configuration INI.

Crypter un mot de passe dans le profil de configuration du serveur

Les nouveaux mots de passe cryptés peuvent être exportés dans le profil de configuration du serveur.

Lors de l'importation d'un profil de configuration de serveur, vous pouvez supprimer les commentaires de l'attribut de mot de passe existant ou du ou des nouveaux attributs de hachage de mot de passe. Si ces deux attributs ne comportent pas de commentaires, une erreur est générée et le mot de passe n'est pas défini. Aucun attribut commenté n'est appliqué lors d'une importation.

Génération de mot de passe crypté sans authentification SNMPv3 et IPMI

Il est possible de générer le mot de passe de hachage sans authentification SNMPv3 et IPMI avec ou sans attribut Salt. Tous deux nécessitent SHA256.

Pour générer un mot de passe de hachage avec l'attribut Salt :

1. Pour les comptes d'utilisateur de l'iDRAC, vous devez générer un mot de passe aléatoire à l'aide de SHA256.
   - Lorsque vous générez le mot de passe avec l'attribut Salt, une chaîne binaire de 16 octets y est ajoutée. L'attribut Salt doit être de 16 octets, s'il est fourni. Une fois ajouté, il prend la forme d'une chaîne de 32 caractères. Le format est « mot de passe » + « attribut Salt », par exemple :
     - Mot de passe = SOMEPASSWORD
     - Salt = ALITTLEBITOFSALT : 16 caractères sont ajoutés.

2. Ouvrez une invite de commande Linux et exécutez les commandes suivantes :

```
Generate Hash-> echo-n SOMEPASSWORDALITTLEBITOFSALT|sha256sum  -><HASH>
```

```
Generate Hex Representation of Salt -> echo -n ALITTLEBITOFSALT | xxd -p   -> <HEX-SALT>
```

```
set iDRAC.Users.4.SHA256Password <HASH>
```

```
set iDRAC.Users.4.SHA256PasswordSalt <HEX-SALT>
```

3. Fournissez la valeur de hachage et l'attribut Salt dans le profil de configuration de serveur importé à l'aide des commandes RACADM ou Redfish.

REMARQUE : Si vous souhaitez effacer un mot de passe précédemment généré avec l'attribut Salt, assurez-vous que le jeu mot de passe-attribut salt est explicitement défini sur une chaîne vide.

```
set iDRAC.Users.4.SHA256Password
ca74e5fe75654735d3b8d04a7bdf5dcdd06f1c6c2a215171a24e5a9dcb28e7a2
```

```
set iDRAC.Users.4.SHA256PasswordSalt
```

4. Après avoir défini le mot de passe, l'authentification du mot de passe en texte clair normal fonctionne, sauf que l'authentification SNMP v3 et IPMI échoue pour les comptes d'utilisateur de l'iDRAC dont les mots de passe ont été mis à jour avec le hachage.

Modification des paramètres du compte d'administrateur local

Après avoir défini l'adresse IP de l'iDRAC, vous pouvez modifier les paramètres du compte d'administrateur local (à savoir, l'utilisateur 2) à l'aide de l'utilitaire de configuration de l'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. Spécifiez les informations pour le **nom d'utilisateur**, les **privilèges de l'utilisateur LAN**, les **privilèges de l'utilisateur du port série** et le **changement du mot de passe**.
   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 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'iDRAC ou de l'utilitaire de configuration d'iDRAC.

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

Pour définir les informations d'emplacement du système :

1. Dans l'interface Web de l'iDRAC, accédez à **Système** > **Détails** > **Détails du système**.
   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'iDRAC**.
3. Cliquez sur **Appliquer**. Les informations d'emplacement du système sont enregistrées dans l'iDRAC.

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

Pour spécifier les détails d'emplacement du système, utilisez les objets du groupe `System.Location`.

Pour plus d’informations, rendez-vous sur le site Guide de la CLI RACADM de l’Integrated Dell Remote Access Controller.

Définition de l'emplacement du système géré à l'aide de l'utilitaire de configuration d'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. Saisissez les informations d’emplacement du système géré dans le datacenter. 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 informations sont enregistrées.

Optimisation des performances du système et de la consommation électrique

L’énergie requise pour refroidir un serveur peut augmenter de manière significative l’énergie totale consommée par le système. La régulation thermique est la gestion active du système de refroidissement au moyen de la vitesse de ventilateur et la gestion de l’alimentation du système, afin de vous assurer que le système est fiable tout en réduisant la consommation électrique du système, la circulation d’air et l’intensité acoustique du système. Vous pouvez régler les paramètres de régulation thermique et les optimiser en fonction des exigences de performances du système et de performances par Watt.

À l’aide de l’interface Web iDRAC, RACADM ou l’utilitaire de configuration d'iDRAC, vous pouvez modifier les paramètres thermiques suivants :

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

Vous trouverez ci-dessous la liste des fonctionnalités de gestion thermique :

- **Consommation de circulation d’air du système** : affiche la consommation de circulation d’air du système en temps réel (en CFM), ce qui permet l’équilibrage de la circulation d’air au niveau du rack et du datacenter.
- **Delta-T personnalisé** : limitez l’élévation de la température de l’air entre l’air aspiré et l’air rejeté pour redimensionner correctement votre système de refroidissement.
- **Contrôle de la température d’évacuation** : spécifiez la limite de température de l’air sortant du serveur pour répondre à vos besoins de datacenter.
- **Température d’entrée PCIe personnalisée** : choisissez la bonne température d’entrée pour répondre aux exigences des appareils tiers.
- **Paramètres de circulation d’air PCIe** : fournit une vue complète du serveur sur le refroidissement des périphériques PCIe et permet la personnalisation du refroidissement des cartes tierces.

Modification des paramètres thermiques à l’aide de l’interface Web iDRAC

Pour modifier les paramètres thermiques :

1. Dans l’interface Web de l’iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Configuration du refroidissement**.

2. Indiquez les informations suivantes :
   - **Optimisation du profil thermique** : sélectionnez le profil thermique :
     - **Paramètres du profil thermique par défaut (puissance minimale)** : implique que l'algorithme thermique utilise les mêmes paramètres de profil système qui sont définis sous la page **BIOS du système** > **Paramètres du BIOS du système** > **Paramètres du profil système**.

     Par défaut, cette option est définie sur **Paramètres du profil thermique par défaut**. Vous pouvez également sélectionner un algorithme personnalisé, indépendant du profil BIOS. Les options disponibles sont les suivantes :
     - **Performances maximales (Performances optimisées)** :
       - Réduction de la probabilité de limitation de la mémoire ou du processeur.
       - Augmentation de la probabilité d'activation du mode Turbo.
       - En général, la vitesse du ventilateur est plus élevée lorsque l'appareil est en veille et en cas de charge de contrainte.

       REMARQUE : La vitesse du ventilateur ne change pas, même lorsque l'option Performances maximales est sélectionnée pour certaines configurations spécifiques.
     - **Puissance minimale (Performance par watt optimisée)** :
       - Optimisé pour la plus faible consommation électrique du système en fonction de l'état optimal de l'alimentation du ventilateur.
       - En règle générale, des vitesses de ventilateur moins élevées à l'état de charges inactif et de contrainte.
     - **Plafond acoustique** : réduit le bruit provenant d'un serveur, mais en limite les performances. L'activation du plafond acoustique peut inclure le déploiement ou l'évaluation temporaire d'un serveur dans un espace occupé, mais cette option ne doit pas être utilisée pendant l'analyse comparative de performance ou lors de l'exécution d'applications sensibles aux performances.

     REMARQUE : La sélection de **Performances maximales** ou de **Puissance minimale** remplace les paramètres thermiques associés au paramètre de profil du système à la page **BIOS du système** > **Paramètres du BIOS système.Paramètres du profil du système**.
   - **Limite de température maximale d'évacuation** : dans le menu déroulant, sélectionnez la valeur maximale de la température de l'air expulsé. Les valeurs sont affichées en fonction du système.

     REMARQUE : La valeur par défaut est **Défaut, 70 °C (158 °F)**.

     Cette option permet au système de modifier la vitesse des ventilateurs de telle manière que la température d'évacuation ne dépasse pas la limite de température d'évacuation sélectionnée. Elle n'est pas toujours garantie dans toutes les conditions de fonctionnement du système d'exploitation en raison d'une dépendance de la charge du système et des capacités de refroidissement du système.
   - **Décalage de la vitesse du ventilateur** : sélectionner cette option permet au serveur d'utiliser des capacités de refroidissement supplémentaires. En cas d'ajout d'un matériel (par exemple, de nouvelles cartes PCIe), des capacités de refroidissement supplémentaires peuvent s'avérer nécessaires. Un décalage de la vitesse du ventilateur entraîne une augmentation de la vitesse des ventilateurs (par la valeur de décalage en %) par rapport aux vitesses de base des ventilateurs calculées par l'algorithme de régulation thermique. Les valeurs possibles sont :
     - **Faible vitesse du ventilateur** : ramène la vitesse des ventilateurs à une vitesse de ventilation modérée.
     - **Vitesse de ventilateur moyenne** : ramène la vitesse des ventilateurs à une vitesse moyenne.
     - **Haute vitesse de ventilateur** : ramène la vitesse des ventilateurs à une vitesse de ventilation maximale.
     - **Vitesse maximale de ventilation** : ramène la vitesse des ventilateurs à la vitesse maximale.
     - **Désactivé** : le décalage de la vitesse du ventilateur est défini sur Désactivé. C'est la valeur par défaut. Lorsque cette option est désactivée, le pourcentage ne s'affiche pas. La vitesse du ventilateur par défaut est appliquée sans décalage. En revanche, le paramètre maximal entraîne l'exécution de tous les ventilateurs à une vitesse maximale.

     REMARQUE :
     - Le décalage de la vitesse de ventilateur est dynamique et dépend du système. L'augmentation de la vitesse de ventilateur à chaque décalage s'affiche en regard de chaque option.
     - Le décalage de la vitesse du ventilateur augmente toutes les vitesses de ventilateur du même pourcentage. Les vitesses de ventilateur peuvent augmenter au-delà des vitesses de décalage en fonction des besoins spécifiques en refroidissement de chaque composant. La consommation électrique globale du système devrait augmenter.
     - Le décalage de vitesse du ventilateur vous permet d'augmenter la vitesse du ventilateur du système en quatre étapes incrémentielles. Ces étapes sont réparties de manière égale entre la vitesse de base standard et la vitesse maximale des ventilateurs du système de serveur. Certaines configurations matérielles entraînent une augmentation de la vitesse de

référence des ventilateurs, ce qui se traduit par des décalages autres que le décalage maximum pour parvenir à la vitesse maximale.

- Le scénario d'utilisation le plus courant est un refroidissement de la carte PCIe non standard. Cependant, la fonctionnalité peut être utilisée pour augmenter le refroidissement du système à d'autres fins.

- **Seuils**
  - **Température maximale d'entrée PCIe** : la valeur par défaut est 55°C. Sélectionnez la température inférieure de 45°C pour les cartes PCIe tierces qui nécessitent une température d'entrée inférieure.
  - **Limites de la température d'évacuation** : en modifiant les valeurs des paramètres suivants vous pouvez définir les limites de la température d'évacuation :
    - **Définir la limite maximale de la température d'évacuation**
    - **Définir la limite de la hausse de la température de l'air**
  - **Vitesse minimale du ventilateur en PMW (% max.)** : sélectionnez cette option pour régler la vitesse du ventilateur. Cette option vous permet d'augmenter la vitesse de référence du ventilateur du système ou d'augmenter la vitesse du ventilateur du système si d'autres options de personnalisation de vitesse du ventilateur n'entraînent pas des vitesses de ventilateur plus élevées.
    - **Valeur par défaut** : définit la vitesse du ventilateur minimale sur la valeur par défaut comme déterminé par l'algorithme de refroidissement du système.
    - **Personnalisé** : saisissez le pourcentage que vous souhaitez appliquer à la vitesse du ventilateur. La plage est comprise entre 9 et 100.

    REMARQUE :
    - La plage autorisée pour une vitesse de ventilateur minimale en PWM est dynamique en fonction de la configuration du système. La première valeur est la vitesse à l'état inactif et la deuxième valeur est la configuration maximale (en fonction de la configuration du système, la vitesse maximale peut être jusqu'à 100 %.).
    - Pour toutes les configurations de stockage SAS/SATA, la vitesse du ventilateur est plafonnée à 95 %.
    - Les ventilateurs du système peuvent fonctionner à une vitesse supérieure à celle-ci en fonction des besoins thermiques du système, mais pas à une vitesse inférieure à la vitesse minimale définie. Par exemple, la définition de la vitesse minimale du ventilateur à 35 % limite la vitesse du ventilateur de façon à ce qu'elle ne tombe jamais en-dessous de 35 % PWM.
    - 0 % PWM n'indique pas que le ventilateur est désactivé. Il s'agit de la vitesse la plus faible que le ventilateur peut atteindre.
    - Sur les serveurs dotés de plusieurs zones, une panne de ventilateur dans l'une des zones telles que le module de processeur hôte (HPM) et la carte mère PCIe (PCB) entraîne le fonctionnement de tous les ventilateurs à une vitesse maximale.

Les paramètres sont persistants, ce qui signifie qu'une fois qu'ils ont été définis et appliqués, ils n'adoptent pas automatiquement la configuration par défaut lors du redémarrage du système, du cycle d'alimentation, de l'iDRAC ou des mises à jour du BIOS. Les options personnalisées de refroidissement ne sont pas forcément prises en charge sur tous les serveurs. Si les options ne sont pas prises en charge, elles ne s'affichent pas ou vous ne pouvez pas fournir une valeur personnalisée.

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

   Le message suivant s'affiche :

   ```
   It is recommended to reboot the system when a thermal profile change has been made. This is to ensure all power and thermal settings are activated.
   ```

4. Cliquez sur **Redémarrer ultérieurement** ou **Redémarrer maintenant**.

REMARQUE : L'activation du ventilateur dépend de l'activation de la configuration thermique appropriée (boucle ouverte), ce qui à son tour dépend des configurations matérielles respectives présentes dans la configuration. Exemple : les disques durs arrière requis.

REMARQUE : Vous devez redémarrer le système pour appliquer les paramètres.

Modification des paramètres thermiques à l'aide de RACADM

Pour modifier les paramètres thermiques, utilisez les objets du groupe **system.thermalsettings** secondaire avec la sous-commande **set**, telle qu'elle est fournie dans le tableau suivant.

Tableau 12. Paramètres thermiques

Objet	Description	Utilisation	Exemple

`AirExhaustTemp`	Permet de définir une limite maximale de température de sortie d'air.	Précisez l'une des valeurs suivantes (selon le système) :
		• 0 : Indique une température de 40 °C
		• 1 : Indique une température de 45 °C
		• 2 : Indique une température de 50 °C
		• 3 : Indique une température de 55 °C
		• 4 : Indique une température de 60 °C
		• 255 : indique une température de 70 °C (par défaut)
			• Pour vérifier le paramètre existant sur le système :
			`racadm get system.thermalsettings.AirExhaustTemp`
			• Le résultat est :
			`AirExhaustTemp=70`
			• Cette sortie indique que le système est configuré pour limiter la température d'échappement de l'air à 70°C. Pour définir la limite de température d'échappement à 60°C :
			`racadm set system.thermalsettings.AirExhaustTemp 4`
			• Le résultat est :
			`Object value modified successfully.`
			• Si un système ne prend pas en charge une limite de température de sortie spécifique, lorsque vous exécutez la commande suivante :
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			• Le message d'erreur suivant s'affiche :
			`ERROR: RAC947: Invalid object value specified.`
			• Assurez-vous de spécifier la valeur en fonction du type d'objet. Pour plus d'informations, consultez l'aide de RACADM. Pour définir la limite par défaut :
			`racadm set system.thermalsettings.AirExhaustTemp 255`

`FanSpeedHighOffsetVal`	• L'obtention de cette variable lit la valeur de décalage de vitesse de ventilateur en %PWM pour le paramètre Décalage de vitesse de ventilateur élevée. • Cette valeur dépend du système. • Utilisez l'objet `FanSpeedOffset` pour définir cette valeur à l'aide de la valeur d'index 1.	Valeurs comprises entre 0 et 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal` Une valeur numérique, par exemple 66, est renvoyée. Cette valeur indique que lorsque vous utilisez la commande suivante, elle applique un décalage de vitesse de

Tableau 12. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple
			ventilateur Élevée (66 % PWM) à la vitesse de ventilateur de référence. `racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	• L'obtention de cette variable lit la valeur de décalage de vitesse de ventilateur en %PWM pour le paramètre Décalage de vitesse de ventilateur faible.
	• Cette valeur dépend du système.
	• Utilisez l'objet `FanSpeedOffset` pour définir cette valeur à l'aide de la valeur d'index 0.
		Valeurs comprises entre 0 et 100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			Ce calcul renvoie une valeur telle que « 23 ». Cela signifie que lorsque vous utilisez la commande suivante, elle applique un décalage de vitesse de ventilateur Faible (23 % PWM) à la vitesse de ventilateur de référence.
			`racadm set system.thermalsettings FanSpeedOffset 0`

`FanSpeedMaxOffsetVal`	• L'obtention de cette variable lit la valeur de décalage de vitesse de ventilateur en %PWM pour le paramètre Décalage de vitesse de ventilateur maximum.
	• Cette valeur dépend du système.
	• Utilisez l'objet `FanSpeedOffset` pour définir cette valeur à l'aide de la valeur d'index 3.
		Valeurs comprises entre 0 et 100	`racadm get system.thermalsettings FanSpeedMaxOffsetVal`
			Ce calcul renvoie une valeur telle que « 100 ». Cela signifie que lorsque vous utilisez la commande suivante, elle applique un décalage de vitesse de ventilateur Maximum (100 % PWM, c'est-à-dire la vitesse maximale). Généralement, ce décalage entraîne une augmentation de la vitesse du ventilateur jusqu'à la vitesse maximale.
			`racadm set system.thermalsettings FanSpeedOffset 3`

`FanSpeedMediumOffsetVal`	• L'obtention de cette variable lit la valeur de décalage de vitesse de ventilateur en %PWM pour le paramètre Décalage de vitesse de ventilateur moyenne.
	• Cette valeur dépend du système.
	• Utilisez l'objet `FanSpeedOffset` pour définir cette valeur à l'aide de la valeur d'index 2.
		Valeurs comprises entre 0 et 100	`racadm get system.thermalsettings FanSpeedMediumOffsetVal`
			Ce calcul renvoie une valeur telle que « 47 ». Cela signifie que lorsque vous utilisez la commande suivante, elle applique un décalage de vitesse de ventilateur Moyenne (47 % PWM) à la vitesse de ventilateur de référence.
			`racadm set system.thermalsettings FanSpeedOffset 2`

Tableau 12. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple

`FanSpeedOffset`	• L'utilisation de cet objet avec la commande get affiche la valeur du Décalage de vitesse de ventilateur existante.
	• L'utilisation de cet objet avec la commande set vous permet de définir la valeur de décalage de vitesse de ventilateur requise.
	• La valeur d'index identifie le décalage à appliquer et les objets `FanSpeedLowOffsetVal`, `FanSpeedMaxOffsetVal`, `FanSpeedHighOffsetVal` et `FanSpeedMediumOffsetVal` (définis antérieurement) sont les valeurs appliquées aux décalages.
		Les valeurs possibles sont les suivantes :
		• 0 : vitesse de ventilateur faible
		• 1 : vitesse de ventilateur élevée
		• 2 : vitesse de ventilateur moyenne
		• 3 : vitesse de ventilateur maximale
		• 255 : aucune
			Pour afficher le paramètre existant :
			`racadm get system.thermalsettings.FanSpeedOffset`
			REMARQUE : Pour définir la valeur du décalage de vitesse de ventilateur sur Élevée (tel que défini dans `FanSpeedHighOffsetVal`)
			`racadm set system.thermalsettings.FanSpeedOffset 1`

`MFSMaximumLimit`	Limite maximum de lecture pour MFS	Valeurs comprises entre 1 et 100	Pour afficher la valeur la plus élevée qui peut être définie à l'aide de l'option `MinimumFanSpeed` : `racadm get system.thermalsettings.MFSMaximumLimit`
`MFSMinimumLimit`	Limite minimum de lecture pour MFS	Valeurs comprises entre 0 et `MFSMaximumLimit` La valeur par défaut est 255 (signifie Aucune)	Pour afficher la valeur la moins élevée qui peut être définie à l'aide de l'option `MinimumFanSpeed`. `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• Permet de configurer la vitesse de ventilateur minimum requise pour que le système puisse fonctionner. • Cette option définit la valeur de ligne de base (standard) de la vitesse de ventilateur et le système autorise une valeur de vitesse de ventilateur plus faible que cette vitesse-là. • Cette valeur est une valeur de %PWM valeur pour la vitesse de ventilateur.	Valeurs comprises entre `MFSMinimumLimit` et `MFSMaximumLimit` Lorsque la commande get indique une valeur de 255, cela signifie que le décalage configuré par l'utilisateur n'est pas appliqué.	Pour vous assurer que la vitesse minimum du système ne tombe pas en dessous de 45 % PWN (45 doit être une valeur comprise entre `MFSMinimumLimit` et `MFSMaximumLimit`) : `racadm set system.thermalsettings.MinimumFanSpeed 45`

Tableau 12. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple

`ThermalProfile`	• Permet de spécifier l'algorithme thermique de base.
	• Permet de définir le profil système, le cas échéant, pour le comportement thermique associé au profil.
		Valeurs :
		• 0 : automatique
		• 1 : performances optimales
		• 2 : alimentation minimum
			Pour afficher le paramètre de profil thermique existant :
			`racadm get system.thermalsettings.ThermalProfile`
			REMARQUE : Pour définir le profil thermique sur Performances maximales :
			`racadm set system.thermalsettings.ThermalProfile 1`

`ThirdPartyPCIFanResponse`	• Contournements thermiques pour les cartes PCI tierces. • Vous permet de désactiver ou d'activer la réponse des ventilateurs système par défaut pour les cartes PCI tierces. • Vous pouvez confirmer la présence d'une carte PCI tierce en affichant l'ID de message PCI3018 dans le journal du Lifecycle Controller.	Valeurs : • 1 – Activé • 0 - Désactivé **REMARQUE :** La valeur par défaut est 1.	Pour désactiver la valeur par défaut de réponse de vitesse du ventilateur définie pour une carte PCI tierce partie détectée : `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

Modification des paramètres thermiques à l'aide de l'utilitaire de paramètres d'iDRAC

Pour modifier les paramètres thermiques :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Thermique**
   La page **Paramètres thermiques iDRAC** s'affiche.
2. Indiquez les informations suivantes :
   - Profil thermique
   - Limite de température maximale d'évacuation
   - Décalage de la vitesse du ventilateur
   - Vitesse minimum du ventilateur

   Les paramètres sont persistants, ce qui signifie qu'une fois qu'ils ont été définis et appliqués, ils n'adoptent pas automatiquement la configuration par défaut lors du redémarrage du système, du cycle d'alimentation, de l'iDRAC ou des mises à jour du BIOS. Certains serveurs Dell peuvent ou non prendre en charge la totalité ou une partie de ces options de refroidissement définies par l'utilisateur. Si les options ne sont pas prises en charge, elles ne s'affichent pas ou vous ne pouvez pas fournir une valeur personnalisée.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres thermiques sont définis.

Modification des paramètres PCIe de circulation de l'air à l'aide de l'interface Web de l'iDRAC

Les paramètres PCIe de circulation de l'air sont utiles lorsque l'augmentation de la marge thermique devient souhaitable pour les cartes PCIe haute puissance personnalisées.

REMARQUE : Les paramètres PCIe de circulation de l'air ne sont pas disponibles pour les disques M.2 connectés via des cartes de montage directes ou BOSS.

Pour modifier les paramètres PCIe de circulation de l'air :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Configuration du refroidissement**.
   La page **Paramètres PCIe de circulation de l'air** s'affiche dans la section des paramètres du ventilateur.
2. Indiquez les informations suivantes :
   - **Mode LFM** : sélectionnez le mode **Personnalisé** pour activer l'option LFM personnalisé.
   - **LFM personnalisé** : saisissez la valeur LFM.
3. Cliquez sur **Appliquer** pour appliquer les paramètres.

   Le message suivant s'affiche :

   ```
   It is recommended to reboot the system when a thermal profile change has been made. This is to ensure all power and thermal settings are activated.
   ```

   Cliquez sur **Redémarrer ultérieurement** ou **Redémarrer maintenant**.

   REMARQUE : Redémarrez le système pour appliquer les modifications.

Installation de la station de gestion

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

Pour installer la station de gestion :

1. Installez un système d'exploitation pris en charge. Pour en savoir plus, voir les notes de mise à jour.
2. Installez et configurez un navigateur Web pris en charge. Pour en savoir plus, voir les notes de mise à jour.
3. À partir du DVD **Dell Systems Management Tools and Documentation**, installez la VMCLI RACADM distante à partir du dossier SYSMGMT. Vous pouvez également exécuter **Setup** sur le DVD pour installer l'interface distante RACADM par défaut et d'autres logiciels OpenManage. Pour en savoir plus sur RACADM, voir Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.
4. Installez les éléments suivants en fonction des besoins :
   - Client SSH
   - TFTP
   - Dell OpenManage Essentials

Accès à distance à l'iDRAC

Pour accéder à distance à l'interface utilisateur de l'iDRAC à partir d'une station de gestion, définissez la carte NIC de l'iDRAC sur **Dédiée** ou **LOM1** pour vous assurer que la station de gestion se trouve sur le même réseau que l'iDRAC.

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

Configuration des navigateurs web pris en charge

REMARQUE : Pour en savoir plus sur les navigateurs pris en charge et leurs versions, consultez le fichier de **Notes de mise à jour**, disponible sur Manuels iDRAC.

La plupart des fonctions de l'interface Web de l'iDRAC sont accessibles en utilisant ces navigateurs avec des paramètres par défaut. Pour que certaines fonctions opèrent, vous devez modifier certains paramètres. Ces paramètres incluent la désactivation des bloqueurs de fenêtres publicitaires, l'activation de la prise en charge du plug-in eHTML5, etc.

Si vous vous connectez à l'interface Web de l'iDRAC depuis une station de gestion qui se connecte à Internet via un serveur proxy, vous devrez configurer le navigateur Web pour qu'il accède à Internet via ce serveur.

REMARQUE : Si vous utilisez Firefox pour accéder à l'interface Web de l'iDRAC, il se peut que vous deviez configurer certains paramètres comme décrit dans cette section. Vous pouvez utiliser d'autres navigateurs pris en charge avec leurs paramètres par défaut.

REMARQUE : Les paramètres de proxy vides sont traités de la même manière que s'il n'y a aucun proxy.

Configuration de Mozilla Firefox

Cette section fournit des détails à propos de la configuration de Firefox pour que vous puissiez accéder à l'interface Web d'iDRAC et utiliser toutes ses fonctionnalités. Ces paramètres sont les suivants :

- Désactivation de la fonction de liste blanche
- Configuration de Firefox pour activer la connexion directe (SSO) Active Directory

REMARQUE : Le navigateur Mozilla Firefox ne possède peut-être pas de barre de défilement pour la page d'aide en ligne d'iDRAC.

Désactivation de la fonction de liste blanche dans Firefox

Firefox dispose d'une fonctionnalité de sécurité de « liste blanche » qui nécessite l'autorisation de l'utilisateur pour installer des plug-ins pour chaque site distinct hébergeant un plug-in. Si elle est activée, la fonctionnalité de liste blanche vous oblige à installer un visualiseur de console virtuelle pour chaque iDRAC que vous visitez, même si les versions du 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 Adresse, saisissez `about:config`, puis appuyez sur la touche 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 remplacées par du texte en gras. La valeur **État** est remplacée par l'utilisateur défini et le champ **Valeur** est défini sur false.
4. Dans la colonne de **Nom de préférence**, recherchez **xpinstall.enabled**.
   Vérifiez que le champ **Valeur** est défini sur **true**. Si ce n'est pas le cas, double-cliquez sur **xpinstall.enabled** pour définir le champ **Valeur** sur **true**.

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 de Firefox, saisissez `about:config`.
2. Dans **Filtrer**, saisissez `network.negotiate`.
3. Ajoutez le nom de domaine à network.negotiate-auth.trusted-uris (en utilisant une liste d'éléments séparés par des virgules).
4. Ajoutez le nom de domaine à network.negotiate-auth.trusted-uris (en utilisant une liste d'éléments séparés par des virgules).

Configuration des navigateurs Web pour utiliser la console virtuelle

REMARQUE : La console virtuelle utilise uniquement eHTML5. Java et ActiveX ne sont plus pris en charge.

Pour utiliser la console virtuelle sur la station de gestion :

1. Assurez-vous qu'une version prise en charge du navigateur (Microsoft Edge ou Mozilla Firefox (Windows ou Linux), Google Chrome, Safari) est installée.

   REMARQUE : Dans le système d'exploitation RHEL avec le navigateur Mozilla, le comportement suivant a été observé lors de la perte du réseau (retrait et réinstallation du câble réseau) :

   - Il arrive que le message de reconnexion ne s'affiche pas dans vConsole tant que le réseau n'est pas opérationnel.
   - Le message contextuel **Connexion refusée** peut s'afficher au lieu du message d'erreur **Échec de la reconnexion** si le réseau est inactif pendant plus de 180 secondes.

REMARQUE : Lors de l'utilisation du navigateur Safari, il est recommandé de désélectionner les options **NSURLSession WebSocket** si elles sont sélectionnées, puis d'ouvrir vConsole. Pour désactiver les options **NSURLSession WebSocket** dans Safari, accédez à **Safari** > **Développer** > **Fonctionnalités expérimentales** > **Fonctionnalités expérimentales**.

Pour plus d'informations sur les versions de navigateur prises en charge, voir les **Notes de mise à jour** disponibles sur Manuels iDRAC.

REMARQUE : Nous vous recommandons de désactiver la fonction de recherche virtuelle dans le navigateur Edge comme bonne pratique. Elle est activée par défaut. Vous risquez d'effectuer une recherche d'images à votre insu. Par conséquent, vous pouvez désactiver ce comportement en configurant les paramètres du navigateur Edge.

2. Pour utiliser Microsoft Edge, configurez le navigateur pour **Exécuter en tant qu'administrateur**.
3. Configurez le navigateur Web pour utiliser le plug-in eHTML5.
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 package associé `compat-libstdc++-33-3.2.3-61` peut être inclus dans le package .NET Framework ou dans le package 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.

Importation de certificats CA vers la station de gestion

Lorsque vous lancez la console virtuelle ou le média virtuel, des invites s'affichent afin de vérifier les certificats. Si vous disposez de certificats de serveur Web personnalisés, vous pouvez éviter ces invites en important les certificats CA dans le magasin de certificats de confiance.

Pour plus d'informations sur l'inscription automatique de certificat (ACE), voir Inscription automatique de certificats.

Importation d'un certificat CA vers le magasin 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** puis 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**, puis sur **OK**. La fenêtre **Panneau de configuration Java** se ferme.

Affichage des versions localisées de l'interface Web

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

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

Les ID ISO entre parenthèses indiquent les variantes linguistiques prises en charge. Pour certaines langues prises en charge, il est nécessaire de redimensionner la fenêtre du navigateur à 1 024 pixels de large pour afficher toutes les fonctionnalités.

L'interface Web de l'iDRAC est conçue pour fonctionner avec les claviers localisés pour les variantes linguistiques prises en charge. Certaines fonctionnalités de l'interface Web de l'iDRAC, telles que la console virtuelle, peuvent nécessiter des étapes supplémentaires pour accéder à certaines fonctions ou lettres. Les autres claviers ne sont pas pris en charge et peuvent entraîner des problèmes inattendus.

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'iDRAC.

Mise à jour de firmware de périphérique

Vous pouvez mettre à jour l'iDRAC, le BIOS et tous les firmwares de périphérique, tels que :

- Cartes Fibre Channel (FC)
- Diagnostics
- Pack de pilotes de système d'exploitation
- Carte d'interface réseau (NIC)
- Contrôleur RAID
- Bloc d'alimentation (PSU)
- Accélérateur (processeur graphique)
- Périphériques PCIe NVMe
- Disques durs SAS/SATA
- Mise à jour du fond de panier des boîtiers internes et externes

PRÉCAUTION : La mise à jour de firmware du bloc d'alimentation peut prendre plusieurs minutes, selon la configuration du système et le modèle de bloc d'alimentation. Pour éviter d'endommager le bloc d'alimentation, n'interrompez pas le processus de mise à jour et ne mettez pas le système sous tension pendant une mise à jour du firmware du bloc d'alimentation.

REMARQUE :

- Le journal LC peut signaler une perte de communication et des messages d'avertissement de restauration lors d'une mise à jour du firmware du processeur graphique.
- Après avoir effectué une mise à jour du firmware du bloc d'alimentation, le système lance un cycle d'alimentation secteur virtuel.

REMARQUE :

- Lorsqu'une mise à jour de firmware est tentée sur un disque enfiché à chaud, un message PR7 dupliqué doit s'afficher dans les journaux Lifecycle.
- Lorsque le statut du journal est **En cours d'exécution** et lorsqu'il n'y a aucune mise à jour du statut à partir des modules de mise à jour, la tâche expire après 6 heures et elle est marquée comme étant en échec.
- Si le statut de la tâche est **En cours d'exécution**, la tâche de mise à jour du firmware peut être marquée **En échec** après le redémarrage de l'iDRAC.
- N'utilisez pas d'adresse IP à partir du site downloads.dell.com lors de l'exécution des mises à jour. Il se peut qu'il ne fonctionne pas comme prévu. Lorsque downloads.dell.com est spécifié comme adresse HTTPS, il n'est pas nécessaire de fournir un chemin d'accès au catalogue. Le catalogue approprié est récupéré automatiquement.

Vous devez charger le firmware requis vers l'iDRAC. Une fois le chargement terminé, la version du firmware actuellement installée sur l'appareil et la version en cours d'application sont affichées. Si la version du firmware en cours d'application n'est pas valide, un message d'erreur s'affiche. Les mises à jour qui ne nécessitent pas un redémarrage prennent effet immédiatement. Les mises à jour qui nécessitent un redémarrage du système sont différées et prévues pour s'exécuter au prochain démarrage du système. Un seul redémarrage du système est requis pour effectuer toutes les mises à jour.

Dans un scénario de mise à jour de firmware en temps réel depuis l'iDRAC, si la tâche est terminée avec un état défini sur **Terminé, CA virtuel en attente**, exécutez le cycle d'alimentation secteur physique ou le cycle d'alimentation secteur virtuel du serveur. Pour un cycle d'alimentation secteur virtuel, utilisez l'URI Redfish ci-dessous. Si une autre méthode est utilisée pour exécuter le cycle d'alimentation secteur, la tâche en temps réel peut échouer. Néanmoins, la version mise à jour reflète toujours le cycle d'alimentation secteur.

REMARQUE :

- Lorsque le mode iLKM est activé sur un contrôleur, la rétrogradation/mise à niveau du firmware de l'iDRAC échoue lorsqu'elle est tentée à partir d'un iLKM vers une version de l'iDRAC non iLKM. La mise à niveau/rétrogradation du firmware de l'iDRAC doit réussir lorsqu'elle est effectuée dans les versions iLKM.
- Lorsque le mode SEKM est activé sur un contrôleur, la rétrogradation/mise à niveau du firmware de l'iDRAC échoue lorsqu'elle est tentée à partir d'une version SEKM vers une version de l'iDRAC non SEKM. La mise à niveau/rétrogradation du firmware de l'iDRAC doit réussir lorsqu'elle est effectuée dans les versions SEKM.
- La rétrogradation du firmware PERC échoue lorsque SEKM est activé.

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

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

- `.exe`: Dell Update Package (DUP) Windows. Vous devez disposer des privilèges de contrôle et de configuration pour pouvoir utiliser ce type de fichier image.
- `.d10`: contient les firmwares de l'iDRAC et du Lifecycle Controller.

Pour les fichiers ayant une extension `.exe`, vous devez disposer du privilège de contrôle du système. La fonctionnalité de mise à jour à distance de firmware et Lifecycle Controller doivent être activés. Cela s'applique à la mise à jour RACADM, à la mise à jour Redfish simple et à la mise à jour de l'interface utilisateur de l'iDRAC.

Pour les fichiers dont l'extension est `.d10`, vous devez disposer des privilèges de configuration. Cela s'applique uniquement à la méthode `racadm fwupdate`.

REMARQUE : Assurez-vous que tous les nœuds du système sont mis hors tension avant de mettre à jour le firmware du bloc d'alimentation

REMARQUE : Après la mise à niveau du firmware de l'iDRAC, il se peut que vous constatiez une différence dans l'horodatage affiché dans le journal du Lifecycle Controller. L'heure affichée dans le journal LC est différente de NTP/BIOS-Time pour quelques journaux pendant la réinitialisation de l'iDRAC.

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

- Téléversement d'un type d'image pris en charge, une à la fois, à partir d'un système local ou un partage réseau.
- Connexion à un site FTP, TFTP, HTTP ou HTTPS ou à une logithèque réseau qui contient les packages DUP Windows et un fichier de catalogue correspondant. Vous pouvez créer des logithèques personnalisées à l'aide de Dell Repository Manager. Pour plus d'informations, reportez-vous au **Guide de l'utilisateur de Dell Repository Manager Data Center**. L'iDRAC peut fournir un rapport sur les différences entre le BIOS et le firmware installés sur le système et les mises à jour disponibles dans le référentiel. Toutes les mises à jour applicables contenues dans le référentiel s'appliquent au système. Cette fonctionnalité est disponible avec la licence iDRAC Enterprise ou Datacenter.

  REMARQUE : Les mises à jour de firmware à l'aide d'un FTP échouent si le proxy HTTP utilisé est configuré sans authentification. Modifiez la configuration du proxy pour autoriser la méthode CONNECT à utiliser des ports non SSL. Par exemple, si vous utilisez un proxy Squid, supprimez la ligne « http_access deny CONNECT !SSL_ports » qui empêche l'utilisation de la méthode CONNECT sur les ports non SSL.

  REMARQUE : Les protocoles HTTP/HTTPS prennent uniquement en charge l'authentification Digest ou aucune authentification.

- Planification des mises à jour automatiques récurrentes du firmware à l'aide du fichier de catalogue et du référentiel personnalisé.

Plusieurs outils et interfaces permettent de mettre à jour le firmware iDRAC. Le tableau suivant s'applique uniquement au firmware iDRAC. Le tableau suivant répertorie les interfaces et les types de fichiers d'image pris en charge. Il indique également si Lifecycle Controller doit être activé pour permettre la mise à jour du firmware.

Tableau 13. Types de fichiers d'image et dépendances

	Image .D10		DUP des iDRAC	
Interface	**Pris en charge**	**Activation de Lifecycle Controller nécessaire**	**Pris en charge**	**Activation de Lifecycle Controller nécessaire**
Mise à jour de RACADM (nouvelle)	Oui	Oui	Oui	Oui
Interface utilisateur des iDRAC	Oui	Oui	Oui	Oui
DUP intrabande du système d'exploitation	Non	S/O	Oui	Non
REMARQUE : Après avoir effectué une mise à jour DUP intrabande, si la mise à jour n'est pas retransmise à l'iDRAC, une tâche Multipart : restauration est créée.				
Redfish	Oui	S/O	Oui	S/O
Diagnostics	Non	Non	Non	Non

Tableau 13. Types de fichiers d'image et dépendances (suite)

Image .D10			DUP des iDRAC	
Interface	**Pris en charge**	**Activation de Lifecycle Controller nécessaire**	**Pris en charge**	**Activation de Lifecycle Controller nécessaire**
Pack de pilotes de système d'exploitation	Non	Non	Non	Non
iDRAC	Oui	Non	Non*	Oui
BIOS	Oui	Oui	Oui	Oui
Contrôleur RAID	Oui	Oui	Oui	Oui
BOSS	Oui	Oui	Oui	Oui
NVDIMM	Non	Oui	Oui	Oui
Fonds de panier	Oui	Oui	Oui	Oui
REMARQUE : Pour les fonds de panier d'extension (actifs), le redémarrage du système est requis.				
Boîtiers	Oui	Oui	Non	Oui
Carte NIC	Oui	Oui	Oui	Oui
Bloc d'alimentation	Oui	Oui	Oui	Oui
REMARQUE : Lorsqu'un redémarrage manuel est effectué ou lorsque la mise à jour est effectuée à partir du système d'exploitation, la mise à jour du bloc d'alimentation nécessite un redémarrage à froid démarrer.				Oui
FPGA	Non	Oui	Oui	Oui
REMARQUE : Une fois que la mise à niveau du firmware FPGA est terminée, l'iDRAC redémarre automatiquement. **REMARQUE :** La mise à jour du référentiel n'est pas prise en charge pour le FPGA lors de l'exécution de la mise à jour FPGA seule ou de la mise à jour FPGA effectuée avec d'autres mises à jour. **REMARQUE :** Lors d'un cycle de marche/arrêt, patientez jusqu'à ce que l'alimentation se décharge (pendant environ 20 secondes) pour vous assurer d'une réinitialisation correcte du système. Sinon, vous pouvez voir LCL et SEL : • SWC9016 : Impossible d'authentifier le FPGA en raison d'un échec de l'authentification cryptographique ou d'un problème d'intégrité. • SWC9018 : Impossible de terminer l'opération de récupération automatique du FPGA en raison d'une erreur interne.				
Cartes FC	Oui	Oui	Oui	Oui
Disques SSD PCIe NVMe	Oui	Non	Oui	Non
Disques durs SAS/ SATA	Non	Oui	Oui	Non
TPM	Non	Oui	Oui	Oui
Application des logiciels et périphériques non SDL	Non	Non	Non	Non

Mise à niveau du firmware à l'aide de l'interface Web d'iDRAC

Utilisez les images du firmware sur le système local ou à partir d'une logithèque sur un partage réseau (CIFS, NFS, HTTP, HTTPS ou FTP).

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

REMARQUE : Assurez-vous que le nom de fichier des DUP de composant unique ne comprend pas d'espace.

Pour mettre à jour le firmware de périphérique à l'aide de l'interface web d'iDRAC :

1. Accédez à **Maintenance** > **Mise à jour du système**. La page **Firmware Update** (Mise à jour de micrologiciel) s'affiche.
2. Sur l'onglet **Mise à jour**, sélectionnez **Local** comme **Type d'emplacement**.

   REMARQUE : Si vous avez sélectionné l'option Local, assurez-vous d'avoir téléchargé l'image de firmware vers un emplacement du système local. Sélectionnez un fichier à préparer à la mise à jour dans iDRAC. Vous pouvez sélectionner des fichiers supplémentaires, un fichier à la fois, pour les télécharger vers l'iDRAC. Les fichiers sont chargés dans un espace temporaire sur iDRAC et limité approximativement à 300 Mo.

3. Cliquez sur **Browse** (Parcourir), sélectionnez le fichier image du micrologiciel pour le composant requis, puis cliquez sur **Upload** (Télécharger). Le firmware requis est téléchargé sur l'iDRAC.
4. Une fois le téléchargement terminé, la section **Update Details** affiche chaque fichier de firmware téléchargé vers l'iDRAC et son état.

   REMARQUE : Si le fichier image du firmware est valide et a été chargé avec succès, la colonne **Contenu** affiche une icône plus (+) à côté du nom du fichier image du firmware. Développez le nom pour afficher les informations **Device Name** (Nom du périphérique), **Current** (En cours) et **Available firmware version** (Version du micrologiciel disponible).

5. Sélectionnez le fichier du micrologiciel requis et effectuez l'une des opérations suivantes :
   - Pour les images de firmware qui ne nécessitent pas un redémarrage du système hôte, cliquez sur **Installer** (seule option disponible). Par exemple, le fichier de firmware de l'iDRAC.
   - Pour les images de micrologiciel qui exigent un redémarrage du système hôte, cliquez sur **Install and Reboot** (Installer et redémarrer) ou **Install Next Reboot** (Installer au prochain redémarrage). Les mises à jour qui nécessitent un redémarrage du système sont différées et prévues pour s'exécuter au prochain démarrage du système. Un seul redémarrage du système est requis pour effectuer toutes les mises à jour.
   - Pour annuler la mise à jour du micrologiciel, cliquez sur **Cancel** (Annuler).

   REMARQUE : Lorsque vous cliquez sur **Installer**, **Installer et redémarrer** ou **Installer au prochain redémarrage**, le message `Updating Job Queue` s'affiche.

6. Pour afficher la page **File d'attente des tâches**, cliquez sur **File d'attente des tâches**. Utilisez cette page pour afficher et gérer les mises à jour différées du firmware ou cliquez sur **OK** pour actualiser la page et afficher l'état de la mise à jour de firmware.

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

   REMARQUE : Vous ne pouvez pas continuer si la session expire après le chargement du fichier de firmware. Seule l'exécution de la commande `reset` de l'interface RACADM peut résoudre ce problème.

   REMARQUE : Une fois la mise à jour du firmware terminée, le message d'erreur suivant s'affiche : `RAC0508: An unexpected error occurred. Wait for few minutes and retry the operation. If the problem persists, contact service provider.` Cela est attendu. Vous pouvez attendre quelques minutes et actualiser le navigateur. Vous êtes alors redirigé vers la page de connexion.

7. Si l'état de la tâche est **Terminé, CA virtuel en attente**, effectuez le cycle d'alimentation CA physique ou le cycle d'alimentation CA virtuel du serveur.

   REMARQUE : Utilisez l'URI Redfish (redfish/v1/Chassis/System.Embedded.1/Actions/Oem/DellOemChassis.ExtendedReset with ResetType=PowerCycle and FinalState=On/Off [pour mettre le système sous tension une fois le VCA terminé ou le laisser à l'état Hors tension]) pour exécuter le cycle d'alimentation virtuel. Si une autre méthode est utilisée pour exécuter le cycle d'alimentation secteur, la tâche en temps réel peut échouer. Néanmoins, la version mise à jour reflète toujours le cycle d'alimentation secteur.

Planification des mises à jour automatiques du firmware

Vous pouvez créer une planification récurrente pour iDRAC afin de rechercher de nouvelles mises à jour de firmware. À la date et à l'heure spécifiées, iDRAC se connecte à la destination spécifiée, recherche les nouvelles mises à jour, et applique ou planifie toutes les mises à jour applicables. Un fichier log est créé sur le serveur distant, qui contient des informations sur l'accès au serveur et les mises à jour de firmware planifiées.

Il est recommandé de créer une logithèque à l'aide de Dell Repository Manager (DRM) et de configurer iDRAC afin d'utiliser cette logithèque pour rechercher et effectuer des mises à jour du firmware. L'utilisation d'une logithèque interne vous permet de contrôler le firmware et les versions disponibles pour iDRAC et permet d'éviter toute modification accidentelle du firmware.

REMARQUE : Pour en savoir plus sur DRM, voir Manuels OpenManage > Repository Manager.

Vous pouvez planifier les mises à jour automatiques du firmware 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 firmware.

Mise à jour de firmware de périphérique à l'aide de RACADM

Pour mettre à jour le firmware de l'appareil à l'aide de RACADM, utilisez la sous-commande `update`. Pour plus d'informations, voir le **Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller** disponible sur Manuels iDRAC.

Exemples :

- Téléchargez le fichier de mise à jour à partir d'un partage HTTP distant :

```
racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share
```

- Téléchargez le fichier de mise à jour à partir d'un partage HTTPS distant :

```
racadm update -f <updatefile> -u admin -p mypass -l https://1.2.3.4/share
```

- 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 référentiel de mise à jour en utilisant `myfile.xml` comme 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 référentiel de mise à jour FTP à l'aide de `Catalog.xml` comme fichier de catalogue :

```
racadm update -f "Catalog.xml" -t FTP -e 192.168.1.20/Repository/Catalog
```

Mise à jour du firmware à l'aide de DUP

Avant de mettre à jour le firmware 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 firmware iDRAC à l'aide de l'utilitaire DUP sous Linux, 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`

Certaines versions des DUP sont conçues d'une telle manière qu'elles entrent en conflit entre elles. Cela se produit au fil du temps, lorsque de nouvelles versions du logiciel sont créées. Une version plus récente du logiciel peut abandonner la prise en charge des périphériques existants. La prise en charge de nouveaux périphériques peut être ajoutée. Considérons, par exemple, les deux DUP Network_Firmware_NDT09_WN64_21.60.5.EXE et Network_Firmware_8J1P7_WN64_21.60.27.50.EXE. Les périphériques pris en charge par ces DUP se divisent en trois groupes.

- Le groupe A correspond aux périphériques existants pris en charge uniquement par NDT09.
- Le groupe B réunit les périphériques pris en charge par NDT09 et 8J1P7.
- Le groupe C rassemble les nouveaux périphériques pris en charge uniquement par 8J1P7.

Prenez l'exemple d'un serveur disposant d'un ou de plusieurs appareils de chacun des groupes A, B et C. Si les DUP sont utilisés un par un, ils doivent réussir. L'utilisation du firmware NDT09 seul met à jour les appareils du groupe A et du groupe B. L'utilisation du firmware 8J1P7 seul met à jour les appareils du groupe B et du groupe C. Toutefois, si vous essayez d'utiliser les deux DUP en même temps, vous

pouvez tenter de créer deux mises à jour pour les appareils du groupe B en même temps. Ces tentatives peuvent échouer et générer une erreur valide : « La tâche pour ce périphérique est déjà présente ». Le logiciel de mise à jour n'est pas en mesure de résoudre le conflit de deux DUP valides lors de deux tentatives de mise à jour valides sur les mêmes périphériques en même temps. Les deux DUP sont par ailleurs nécessaires pour prendre en charge les périphériques du groupe A et du groupe C. Le conflit se prolonge également pour effectuer des restaurations à un point antérieur sur les périphériques. Pour des pratiques optimales, il est recommandé d'utiliser chaque DUP individuellement.

Pour mettre à jour iDRAC à l'aide de 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 firmware 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 micrologiciel à l'aide de l'interface RACADM

1. Téléchargez l'image du micrologiciel sur le serveur TFTP ou FTP. Par exemple : `C:\downloads\firmimg.d10`
2. Exécutez la commande RACADM suivante :

   TFTP server:

   - À l'aide de la commande `fwupdate` :

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -g -u -a <path>
     ```

     path

     l'emplacement sur le serveur TFTP où est stocké `firmimg.d10`.
   - À l'aide de la commande `update` :

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

   FTP server:

   - À l'aide de la commande `fwupdate` :

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate –f <ftpserver IP>
     <ftpserver username> <ftpserver password> -d <path>
     ```

     path

     l'emplacement sur le serveur FTP où est stocké `firmimg.d10`.
   - À l'aide de la commande `update` :

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

   Pour en savoir plus, voir le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Mises à jour sans redémarrage

L'iDRAC prend en charge les mises à jour sans redémarrage. Cette fonctionnalité vous permet d'effectuer la mise à jour du firmware à partir de l'iDRAC sans avoir à redémarrer le serveur hôte pour lancer et effectuer la mise à jour dans l'environnement pré-SYSTÈME D'EXPLOITATION. Afin de déterminer si le DUP prend ou non en charge la mise à jour de bande latérale, des balises permettent d'identifier si le firmware du DUP prend en charge la mise à jour directe de la bande latérale (PLDM, NVMe-MI, etc.) et/ou la méthode de mise à jour UEFI FMP et le type de charge utile présente au sein du DUP.

Lorsque l'iDRAC fait l'inventaire des composants, il détermine si le composant spécifique prend en charge la mise à jour de bande latérale directe ou la mise à jour héritée basée sur le UEFI FMP, et s'il nécessite ou non un redémarrage de l'hôte.

REMARQUE : Pour certains appareils tels que les adaptateurs réseau, un cycle d'alimentation peut être nécessaire pour une mise à jour du firmware.

Deux propriétés spécifiques aux fonctionnalités de mise à jour du firmware PLDM sont consignées lors de l'inventaire logiciel : **PLDMCapabilitiesDuringUpdate** et **PLDMFDPCapabilitiesDuringUpdate**. Ces paramètres sont disponibles uniquement pour les périphériques qui prennent en charge la mise à jour du firmware PLDM.

REMARQUE : La fonction de mise à jour basée sur PLDM est prise en charge uniquement sur les plateformes dotées d'une mémoire iDRAC de 1 Go.

Les modules de mise à jour iDRAC/LC gèrent les méthodes de mise à jour avec ou sans redémarrage selon la prise en charge. Ci-dessous sont répertoriées les différentes méthodes de mise à jour :

- Mise à jour de bande latérale directe avec redémarrage identifié à l'exécution
- Mises à jour de bande latérale directe sans redémarrage
- Mise à jour SSM (basée sur UEFI FMP)/basée sur SMA
- Mise à jour du FPGA Redstone à partir de l'iDRAC
- Mise à jour FPGA à partir de l'iDRAC

REMARQUE : En cas de mises à jour du référentiel, les mises à jour d'application qui ne nécessitent pas de redémarrage de l'hôte doivent être effectuées immédiatement.

REMARQUE : Pour les mises à jour directes (mises à jour du firmware en temps réel) à partir de l'iDRAC, il existe un LCLOG (SUP200, SUP0518, SUP516) avec une description du périphérique (informations FQDD conviviales) au lieu de la description du produit.

REMARQUE : Lorsque les disques NVMe se trouvent derrière PERC (à l'avant) et sont directement connectés au fond de panier arrière ou inversement, la mise à jour sans redémarrage ne fonctionne pas pour les disques à connexion directe.

REMARQUE : Si vous effectuez des mises à jour du firmware en utilisant l'interface utilisateur de LC pour les composants de stockage capables d'effectuer des mises à jour sans redémarrage, ces mises à jour échouent. Par conséquent, utilisez les interfaces de l'iDRAC pour toutes les mises à jour du firmware.

Affichage et gestion des mises à jour planifiées

Vous pouvez afficher et supprimer les tâches planifiées, y compris les tâches de configuration et de mise à jour. Il s'agit d'une fonctionnalité sous licence. Toutes les tâches prévues pour exécution lors du prochain démarrage peuvent être supprimées.

REMARQUE : Si une mise à jour ou d'autres travaux et tâches sont en cours, ne redémarrez pas ou n'arrêtez le système ou n'effectuez pas de cycle d'alimentation CA de l'hôte ou de l'iDRAC via n'importe quel mode (manuel ou en appuyant sur « Ctrl+Alt+Suppr » ou autre dans les interfaces de l'iDRAC). Le système (hôte et iDRAC) doit toujours être redémarré ou arrêté normalement lorsqu'aucune tâche n'est en cours d'exécution dans l'iDRAC ou l'hôte. Un arrêt anormal ou une opération interrompue peut avoir des conséquences imprévisibles, telles que la corruption du firmware, générer des fichiers noyaux, des RSOD, des YSOD, des événements d'erreur dans LCL, etc.

REMARQUE : Pour toute mise à jour nécessitant une réinitialisation/redémarrage de l'iDRAC ou si l'iDRAC est redémarré, il est recommandé de vérifier si l'iDRAC est prêt en attendant quelques secondes, avec un délai d'expiration maximum de 5 minutes, avant d'utiliser une autre commande.

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

Pour afficher les mises à jour différées à l'aide de RACADM, utilisez la sous-commande `jobqueue`. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Affichage et gestion des mises à jour intermédiaires à l'aide de l'interface Web d'iDRAC

Pour afficher la liste des tâches planifiées à l'aide de l'interface Web de l'iDRAC, accédez à **Maintenance** > **File d'attente des tâches**. La page **File d'attente des tâches** affiche l'état des tâches dans la file d'attente de Lifecycle Controller. Pour plus d'informations sur les champs affichés, voir l'**Aide en ligne de l'iDRAC**.

Pour supprimer une ou plusieurs tâches, sélectionnez-les et cliquez sur **Supprimer**. Cette page est actualisée et la tâche sélectionnée est supprimée de la file d'attente de tâches du Lifecycle Controller. Vous pouvez supprimer toutes les tâches en file d'attente prévues pour s'exécuter lors du prochain redémarrage. Vous ne pouvez pas supprimer des tâches actives, c'est-à-dire dont l'état est **En cours d'exécution** ou **En cours de téléchargement**.

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

Restauration du firmware du périphérique

Vous pouvez restaurer le firmware d'iDRAC ou tout périphérique pris en charge par Lifecycle Controller, même si la mise à niveau a été précédemment effectuée à l'aide d'une autre interface. Par exemple, si le firmware a été mis à niveau à l'aide de l'interface utilisateur de Lifecycle Controller, vous pouvez restaurer le firmware à l'aide de l'interface Web d'iDRAC. Vous pouvez effectuer la restauration du firmware pour plusieurs périphériques en un seul démarrage du système.

Il est recommandé de garder le firmware à jour pour vous assurer que vous disposez des dernières fonctions et mises à jour de sécurité. Restaurez ou installez une version antérieure si vous rencontrez des problèmes après une mise à jour. Pour installer une version antérieure, utilisez Lifecycle Controller pour rechercher des mises à jour et sélectionnez la version que vous souhaitez installer.

Vous pouvez effectuer la restauration du firmware sur les composants suivants :

- Integrated Dell Remote Access Controller
- BIOS
- Carte d'interface réseau (NIC)
- Bloc d'alimentation (PSU)
- Contrôleur de stockage
- Fond de panier
- Mémoire permanente software-defined (SDPM)

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

Avant de procéder à une restauration du firmware, assurez-vous que :

- Vous disposez des droits de configuration nécessaires pour restaurer le firmware d'iDRAC.
- Vous disposez des droits de contrôle du serveur et avez activé le Lifecycle Controller pour la restauration de firmware d'un périphérique autre que l'iDRAC.
- Faire passer le mode NIC à **Dédié** si le mode est défini sur **LOM partagé**.

Vous pouvez restaurer la version précédente du firmware en utilisant n'importe laquelle des méthodes suivantes :

- Interface web iDRAC
- Interface Web OME-Modular
- CLI RACADM d'iDRAC
- UI de Lifecycle Controller
- API Redfish

Restauration du firmware à l'aide de l'interface Web d'iDRAC

Pour restaurer un firmware de périphérique :

1. Dans l'interface Web de l'iDRAC, accédez à **Maintenance** > **Mise à jour du système** > **Restauration**.
   La page **Restauration** affiche les appareils dont vous pouvez restaurer le firmware. Vous pouvez afficher le nom du périphérique, la version du firmware actuellement installée, ainsi que la version de restauration du firmware disponible.
2. Sélectionnez un ou plusieurs appareils pour lesquels vous voulez restaurer le firmware.
3. Selon les périphériques sélectionnés, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**. Si vous ne sélectionnez que l'iDRAC, cliquez sur **Installer**.
   Lorsque vous cliquez sur **Installer et redémarrer** ou sur **Installer lors du prochain démarrage**, le message « Mise à jour de la file d'attente de tâches en cours » s'affiche.
4. Cliquez sur **File d'attente des tâches**.
   La page **File d'attente de tâches** s'affiche, dans laquelle vous pouvez afficher et gérer les mises à jour de firmware planifiées.

   REMARQUE :
   - Lorsque la restauration est en cours, le processus de restauration continue de s'exécuter en arrière-plan, même si vous quittez la page.

   Un message d'erreur s'affiche si :

- Vous ne disposez pas des droits de contrôle du serveur pour restaurer des firmwares autres que l'iDRAC ou des privilèges de configuration pour restaurer le firmware de l'iDRAC.
- La restauration de firmware 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 firmware 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 à l'aide de l'interface RACADM

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

   ```
   racadm swinventory
   ```

   Pour le périphérique dont vous voulez restaurer le micrologiciel, l'option `Rollback Version` doit être `Available`. Prenez également note du FQDD.

2. Restauration du micrologiciel du périphérique à l'aide de :

   ```
   racadm rollback <FQDD>
   ```

   Pour en savoir plus, voir Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Restauration facile

La fonction Easy Restore utilise la mémoire flash Easy Restore pour sauvegarder les données. Lorsque vous remplacez le module de contrôle sécurisé (SCM) et mettez le système sous tension, le BIOS interroge l'iDRAC et vous invite à restaurer les données sauvegardées. Le premier écran du BIOS vous invite à restaurer le numéro de série, les licences et les applications de diagnostic UEFI. Le second écran du BIOS vous invite à restaurer les paramètres de configuration du système. Si vous choisissez de ne pas restaurer les données sur le premier écran du BIOS et ne définissez pas le numéro de série à l'aide d'une autre méthode, le premier écran du BIOS s'affiche alors à nouveau. Le second écran du BIOS s'affiche une seule fois.

REMARQUE :

- Les paramètres de configuration système sont sauvegardés uniquement lorsque l'option Collecter l'inventaire système au redémarrage (CSIOR) est activée. Assurez-vous que Lifecycle Controller et la fonction CSIOR sont activés.
- Easy Restore ne sauvegarde pas les autres données, telles que les images du firmware ou celles des cartes d'extension.
- Le remplacement du module de mémoire du processeur hôte (HPM) ne lance pas le processus Easy Restore.

REMARQUE : Lors du remplacement du SCM, vous devez sélectionner manuellement **Refroidissement liquide** ou **Refroidissement à air**. Une mauvaise sélection de ces options entraîne des problèmes thermiques au sein de la plateforme. Le cas échéant, contactez le support technique Dell afin de connaître la procédure de récupération.

Après avoir remplacé la carte système de votre serveur, Easy Restore vous permet de restaurer automatiquement les données suivantes :

- Étiquette de service du système
- Numéro d'inventaire
- Les données des licences
- L'application de diagnostics UEFI
- Les paramètres de configuration du système (BIOS, iDRAC)
- Journal des événements système (SEL)
- Module OEM ID

Vous trouverez ci-dessous les détails de durée requise pour certaines actions de restauration :

- La restauration du contenu du système tel que Diagnostics, Journal des événements système (SEL) et le module OEM ID prend généralement moins d'une minute.
- La restauration des données de configuration système (iDRAC, BIOS) peut prendre plusieurs minutes (dans certains cas environ 10 minutes).

REMARQUE : Pendant ce temps, il n'y a pas d'indication ou de barre de progression et le serveur peut être redémarré plusieurs fois pour terminer la restauration de la configuration.

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

Vous pouvez détecter et surveiller l'iDRAC à l'aide de Dell Management Console ou de Dell OpenManage Essentials. Vous pouvez également utiliser l'outil Dell Remote Access Configuration Tool (DRACT) pour détecter les iDRAC, mettre à jour le firmware et configurer Active Directory. Pour plus d'informations, voir les guides de l'utilisateur respectifs.

Prise en charge de Server Configuration Profile – Importation et exportation

Server Configuration Profile (SCP) vous permet d'importer et d'exporter des fichiers de configuration de serveur.

REMARQUE : Vous devez disposer des droits d'administrateur pour pouvoir effectuer une tâche d'exportation et d'importation SCP.

REMARQUE : Licence Enterprise ou Datacenter requise pour effectuer l'importation SCP. Avec la licence Core, vous pouvez uniquement effectuer une exportation SCP.

Vous pouvez réaliser ces importations/exportations depuis une station de gestion locale ou un partage réseau via CIFS, NFS, HTTP ou HTTPS. Avec SCP, vous pouvez sélectionner et importer/exporter des configurations au niveau des composants pour le BIOS, la carte NIC et le système RAID. Vous pouvez importer et exporter SCP vers la station de gestion locale ou vers un partage réseau CIFS, NFS, HTTP ou HTTPS. Vous pouvez importer ou exporter les profils individuels du contrôleur iDRAC, du BIOS, de la carte NIC et du RAID, ou tous les profils réunis dans un seul fichier.

Vous pouvez spécifier un aperçu de l'importation/exportation du SCP, avec exécution de la tâche et génération du résultat de la configuration, mais sans que la configuration soit appliquée.

Une tâche est créée une fois que l'importation/exportation est initiée au niveau de l'interface utilisateur. L'état des tâches est disponible sur la page « Job Queue » (File d'attente des tâches).

REMARQUE :

- Seuls le nom de l'hôte ou les adresses IP sont acceptés comme adresse de destination.
- Vous pouvez parcourir vos dossiers jusqu'à un emplacement spécifique pour importer les fichiers de configuration de serveur. Sélectionnez le bon fichier de configuration de serveur pour l'importation. Par exemple, importation.xml.
- Selon le format de fichier exporté (que vous avez sélectionné), l'extension est ajoutée automatiquement. Par exemple, `export_system_config.xml`.
- Lors de l'exportation, le nom du fichier SCP peut changer. Par exemple, il peut passer de con.xml à _con.xml.
- SCP applique la configuration complète dans un travail unique et avec un minimum de redémarrages. Cependant, dans quelques configurations système, certains attributs modifient le mode de fonctionnement d'un périphérique ou créent des sous-unités avec de nouveaux attributs. Lorsque cela se produit, le SCP risque de ne pas pouvoir appliquer tous les paramètres au cours d'un travail unique. Passez en revue les entrées ConfigResult pour le travail afin de résoudre les paramètres de configuration éventuellement en attente.
- Pour vous assurer que les rôles d'utilisateur sont importés correctement, définissez la valeur **PasswordHashSaltset** et la valeur **Set on Import** sur **true** dans le fichier d'exportation SCP.

SCP vous permet d'effectuer le déploiement du système d'exploitation (OSD) à l'aide d'un seul fichier xml/json sur plusieurs systèmes. Vous pouvez également effectuer des opérations existantes, telles que les configurations et les mises à jour des référentiels en une seule fois.

SCP permet également d'exporter et d'importer des clés publiques SSH pour tous les utilisateurs iDRAC. Il existe 4 clés publiques SSH pour tous les utilisateurs.

Vous trouverez ci-dessous les étapes de déploiement du système d'exploitation à l'aide de SCP :

1. Exporter un fichier SCP
2. Le fichier SCP contient tous les attributs supprimés nécessaires à l'OSD.

3. Modifiez ou mettez à jour les attributs OSD, puis effectuez l'opération d'importation.
4. Ces attributs OSD sont ensuite validés par l'orchestrateur SCP.
5. L'orchestrateur SCP effectue les mises à jour de la configuration et des référentiels spécifiés dans le fichier SCP.
6. Une fois la configuration et les mises à jour terminées, le système d'exploitation de l'hôte s'arrête.

REMARQUE : Seuls les partages CIFS et NFS sont pris en charge pour l'hébergement des supports du système d'exploitation.

7. L'orchestrateur SCP lance l'OSD en associant les pilotes du système d'exploitation sélectionné, puis lance un démarrage unique sur le support du système d'exploitation présent dans NFS/Share.
8. LCL indique la progression de la tâche.
9. Une fois que le BIOS démarre à partir du support du système d'exploitation, la tâche SCP s'affiche comme étant effectuée.
10. Le support connecté et le support du système d'exploitation sont automatiquement déconnectés après 65 535 secondes ou après la durée spécifiée par l'attribut `OSD.1#ExposeDuration`.

Pour obtenir des informations détaillées sur l'ensemble de la fonctionnalité et le workflow de déploiement, voir la section Utilisation des profils de configuration de serveur pour déployer des systèmes d'exploitation sur des serveurs Dell PowerEdge.

Pour en savoir plus sur SCP, reportez-vous au Guide de référence : Profils de configuration de serveur.

Importation d'un profil de configuration de serveur à l'aide de l'interface Web de l'iDRAC

Avant d'importer le fichier SCP, il est recommandé d'effectuer l'opération d'aperçu d'importation. Cette opération permet d'identifier les problèmes potentiels de format ou les paramètres d'attribut non valides sans affecter l'état du serveur.

Pour importer le profil de configuration de serveur :

1. Accédez à **Configuration** > **Profil de configuration de serveur**.
   La page **Profil de configuration de serveur** s'affiche.
2. Sélectionnez un des éléments suivants pour spécifier le type d'emplacement :
   - **Local** pour importer le fichier de configuration enregistrée sur un disque local.
   - **Partage réseau** pour importer le fichier de configuration à partir du partage CIFS ou NFS.
   - **HTTP ou HTTPS** pour importer le fichier de configuration à partir d'un fichier local à l'aide du transfert de fichiers HTTP ou HTTPS.

   REMARQUE : En fonction du type d'emplacement, vous devez saisir les paramètres réseau ou les paramètres HTTP ou HTTPS. Si le proxy est configuré pour HTTP/HTTPS, les paramètres de proxy sont également obligatoires.
3. Sélectionnez les composants répertoriés dans l'option **Importer des composants**.
4. Sélectionnez le type d'**arrêt**.
5. Sélectionnez le **Temps d'attente maximum** pour spécifier le temps d'attente avant l'arrêt du système une fois l'importation terminée.
6. Cliquez sur **Importer**.

Exportation d'un profil de configuration de serveur à l'aide de l'interface Web de l'iDRAC

Pour exporter le profil de configuration de serveur :

1. Accédez à **Configuration** > **Profil de configuration de serveur**
   La page **Profil de configuration de serveur** s'affiche.
2. Cliquez sur **Exporter**.
3. Sélectionnez un des éléments suivants pour spécifier le type d'emplacement :
   - **Local** pour enregistrer le fichier de configuration sur un disque local.
   - **Partage réseau** pour enregistrer le fichier de configuration sur un partage CIFS ou NFS.
   - **HTTP ou HTTPS** pour enregistrer le fichier de configuration sur un fichier local à l'aide d'un transfert de fichier HTTP/HTTPS.

   REMARQUE : En fonction du type d'emplacement, vous devez saisir les paramètres réseau ou HTTP/HTTPS. Si le proxy est configuré pour HTTP/HTTPS, les paramètres de proxy sont également obligatoires.
4. Sélectionnez les composants pour lesquels vous devez sauvegarder la configuration.
5. Sélectionnez le **Type d'exportation**. Les options sont les suivantes :

- **Basic** : permet de créer un snapshot non destructeur de la configuration.
- **Exportation de remplacement** : remplace les paramètres du serveur par de nouveaux paramètres ou restaure les paramètres du serveur vers une ligne de base connue.
- **Clone Export** : permet de cloner les paramètres d'un serveur vers un autre serveur avec un matériel identique. Tous les paramètres, à l'exception de l'identité d'E/S, sont mis à jour. Les paramètres de cette exportation sont destructifs lorsqu'ils sont téléchargés sur un autre système.

6. Sélectionnez un **Format du fichier d'exportation**.
7. Sélectionnez des **Éléments d'exportation supplémentaires**.
8. Cliquez sur **Exporter**.

Configuration de Secure Boot à l'aide des paramètres du BIOS ou de F2

Secure Boot UEFI est une technologie qui élimine un vide de sécurité majeur qui peut se produire au cours d'un transfert entre le firmware UEFI et le système d'exploitation UEFI (système d'exploitation). Dans le cadre de Secure Boot UEFI, chaque composant de la chaîne a été validé et autorisé par rapport à un certificat spécifique avant qu'il soit autorisé à se charger ou s'exécuter. Secure Boot supprime la menace et fournit la vérification d'identité du logiciel à chaque étape du démarrage : firmware de la plateforme, cartes d'option et chargeur de démarrage du système d'exploitation.

Le forum UEFI (Unified Extensible Firmware Interface), un organisme de l'industrie qui développe des normes pour les logiciels de pré-démarrage, définit Secure Boot dans la spécification UEFI. Les fournisseurs de systèmes informatiques, de cartes d'extension et de systèmes d'exploitation collaborent sur cette spécification pour promouvoir l'interopérabilité. En tant que composant de la spécification UEFI, Secure Boot représente une norme à l'échelle de l'industrie pour la sécurité dans l'environnement de pré-démarrage.

Lorsqu'il est activé, Secure Boot empêche le chargement des pilotes de périphériques UEFI non signés, affiche un message d'erreur et ne permet pas au périphérique de fonctionner. Vous devez désactiver Secure Boot pour charger les pilotes de périphérique non signés.

Formats de fichier acceptables

La stratégie Secure Boot ne contient qu'une clé dans PK, mais plusieurs clés peuvent résider dans KEK. Idéalement, le fabricant ou le propriétaire de la plate-forme conserve la clé privée correspondant à la clé publique PK. Les tiers (tels que les fournisseurs de systèmes d'exploitation et les fournisseurs de périphériques) conservent les clés privées correspondant aux clés publiques dans KEK. De cette manière, les propriétaires de la plate-forme ou les tiers peuvent ajouter ou supprimer des entrées dans la base de données ou la base de données des signatures interdites d'un système spécifique.

La stratégie Secure Boot utilise la base de données et la base de données des signatures interdites pour autoriser l'exécution du fichier image de pré-démarrage. Pour exécuter un fichier image, associez-le à une clé ou une valeur de hachage dans la base de données. Ne l'associez pas à une clé ou une valeur de hachage dans la base de données des signatures interdites. Toute tentative de mise à jour du contenu de la base de données ou de la base de données des signatures interdites doit être signée par une clé KEK ou PK privée. Toute tentative de mise à jour du contenu de PK ou KEK doit être signée par une clé PK privée.

Tableau 14. Formats de fichier acceptables

Composant de stratégie	Formats de fichier acceptables	Extensions de fichier acceptables	Nombre max. d'enregistrements autorisé
PK	Certificat X.509 (format DER binaire uniquement)	1. `.cer` 2. `.der` 3. .crt	un
KEK	Certificat X.509 (format DER binaire uniquement) Magasin de clés publiques	1. `.cer` 2. `.der` 3. `.crt` 4. `.pbk`	Plusieurs

Tableau 14. Formats de fichier acceptables (suite)

Composant de stratégie	Formats de fichier acceptables	Extensions de fichier acceptables	Nombre max. d'enregistrements autorisé
DB et disque dur (DBX)	Certificat X.509 (format DER binaire uniquement) Image EFI (le BIOS du système calcule et importe le condensat d'image)	1. `.cer` 2. `.der` 3. `.crt` 4. `.efi`	Plusieurs

La fonctionnalité Paramètres Secure Boot est accessible en cliquant sur Sécurité du système sous Paramètres du BIOS du système. Pour accéder à Paramètres du BIOS du système, appuyez sur la touche F2 lorsque le logo de la société s'affiche lors de l'auto-test de démarrage.

- Par défaut, Secure Boot est désactivé et la stratégie Secure Boot est définie sur Standard. Pour configurer la stratégie Secure Boot, vous devez activer Secure Boot.
- Lorsque le mode Secure Boot est défini sur Standard, cela indique que le système dispose de certificats par défaut et de condensats d'image ou une valeur de hachage chargés en usine. Cela permet d'assurer la sécurité des micrologiciels standard, des pilotes, des ROM optionnelles et des chargeurs de démarrage.
- Pour prendre en charge un nouveau pilote ou firmware sur un serveur, le certificat correspondant doit être inscrit dans la base de données du magasin de certificats Secure Boot. Par conséquent, la stratégie Secure Boot doit être définie sur Personnalisée.

Lorsque la stratégie Secure Boot est définie sur Personnalisée, elle hérite des certificats standard et des condensats d'image chargés dans le système par défaut, que vous pouvez modifier. La stratégie Secure Boot définie sur Personnalisée vous permet d'effectuer les opérations telles qu'Afficher, Exporter, Importer, Supprimer, Supprimer tout, Réinitialiser et Réinitialiser tout. Ces opérations vous permettent de configurer les stratégies Secure Boot.

Le fait de définir la stratégie Secure Boot sur Personnalisée active les options permettant de gérer le magasin de certificats en utilisant différentes actions, telles qu'Exporter, Importer, Supprimer, Supprimer tout, Réinitialiser et Réinitialiser tout sur PK, KEK, base de données et DBX. Vous pouvez sélectionner la stratégie (PK/KEK/DB/DBX) sur laquelle vous souhaitez effectuer le changement et réaliser les actions requises en cliquant sur le lien correspondant. Chaque section comporte des liens permettant d'effectuer les opérations Importer, Exporter, Supprimer et Réinitialiser. Les liens sont activés en fonction de ce qui est applicable, ce qui dépend de la configuration actuelle. Les opérations Supprimer tout et Réinitialiser tout sont celles qui ont un impact sur toutes les stratégies. L'option Supprimer tout permet de supprimer tous les certificats et tous les condensats d'image dans la stratégie personnalisée, et l'option Réinitialiser tout de restaurer tous les certificats et les condensats d'image du magasin de certificats standard ou par défaut.

Récupération du BIOS

La fonction de récupération du BIOS vous permet de récupérer manuellement le BIOS à partir d'une image enregistrée. Le BIOS est vérifié lors de la mise sous tension du système. S'il est corrompu ou compromis, un message d'erreur s'affiche. Vous pouvez alors lancer le processus de récupération du BIOS à l'aide de RACADM et de Redfish. Pour effectuer une récupération manuelle du BIOS, voir le iDRAC RACADM Command Line Interface Reference Guide (Guide de référence de l'interface de ligne de commande RACADM d'iDRAC), disponible à l'adresse Manuels iDRAC.

Restauration d'iDRAC

iDRAC prend en charge deux images système afin de toujours être amorçable. Lors d'une erreur catastrophique imprévue lorsque vous perdez les deux chemins de démarrage, le chargeur de démarrage de l'iDRAC détecte qu'il n'y a pas d'image amorçable. Le chargeur de démarrage affiche les premiers messages vidéo de démarrage sur l'écran connecté.

Pour restaurer l'iDRAC, effectuez les étapes suivantes :

1. Formatez un lecteur USB avec FAT32 s'il s'agit d'un système d'exploitation Windows ou avec EXT3 ou EXT4 s'il s'agit d'un système d'exploitation Linux.
2. Copiez le fichier **firmimg.d10** ou DUP.exe dans l'emplacement du lecteur USB **/scm/images/** .
3. Insérez la clé USB dans le port USB supérieur arrière du serveur et effectuez un cycle d'alimentation secteur sur le serveur. Le chargeur de démarrage détecte la clé USB, lit le contenu, reprogramme l'iDRAC, puis redémarre l'iDRAC.

5

Unité de traitement des données (DPU)

Une unité de traitement des données (DPU) est un système sur une puce composé de cœurs ARM, d'une carte NIC ASIC et de moteurs d'accélération. Programmable, elle est potentiellement capable d'exécuter un système d'exploitation. Les DPU associent connectivité réseau et cœurs de CPU indépendants de l'hyperviseur ou du système d'exploitation afin d'accélérer et de décharger les services. Les DPU se distinguent des moteurs de déchargement traditionnels par leur flexibilité, leur programmabilité et leur capacité d'hébergement d'un vaste éventail de services.

REMARQUE : Les DPU nécessitent une licence iDRAC10 Enterprise ou Datacenter.

L'utilisation d'une DPU offre les avantages suivants :

- isole les services d'infrastructure du système d'exploitation et des applications de l'hôte ;
- permet à un environnement de fournir de nouveaux services indépendamment de l'environnement applicatif de l'hôte ;
- offre une accélération matérielle permettant de traiter des opérations gourmandes en données à une vitesse similaire à celle d'une connexion filaire ;
- libère des cœurs de processeur serveur/x86 afin de permettre la prise en charge par les applications clients de plateformes edge à socket unique et à format compact.

Une fois le système d'exploitation de la DPU démarré, des fonctions PCIe supplémentaires peuvent être initialisées. Par conséquent, l'énumération PCIe du BIOS (tout comme le processus de démarrage du système d'exploitation/hyperviseur de l'hôte) ne doit se produire qu'une fois le système d'exploitation de la DPU démarré ou prêt.

L'iDRAC vous permet de configurer les paramètres du mode DPU OS Ready (synchronisation du démarrage) sur chaque logement compatible avec la DPU. Les valeurs possibles sont :

- **Activé :** la DPU participe à la réalisation de l'énumération PCIe du BIOS et du processus de démarrage du système d'exploitation/hyperviseur de l'hôte.
- **Désactivé :** la DPU ne participe pas à la réalisation de l'énumération PCIe du BIOS et du processus de démarrage du système d'exploitation/hyperviseur de l'hôte.

Points à prendre en considération concernant la DPU :

- Seuls quelques logements sont compatibles avec la DPU. L'iDRAC vous permet de configurer la synchronisation du démarrage de la DPU par rapport à ces logements uniquement.
- Les paramètres de synchronisation du démarrage de la DPU sont basés sur les logements (et non sur l'identité). Cela signifie que si le périphérique de DPU est déplacé vers un autre logement, il se comportera conformément à la configuration du logement dans lequel il aura été nouvellement inséré.
- Les paramètres de synchronisation du démarrage de la DPU sont configurables même en l'absence de tout périphérique de DPU.
- Après détection, si aucun périphérique de DPU n'est installé dans le logement, les configurations de synchronisation du démarrage de la DPU ne rentrent PAS en vigueur.
- Chaque procédure DPU OS Ready individuelle et la procédure DPU OS Ready globale sont consignées au LCL.
- En cas d'effacement du système sur une plateforme DPU non prise en charge, les journaux LC de la DPU affichent le message SYS560 (`some of the DPU devices failed to reset`). En cas d'effacement du système sur une plateforme DPU prise en charge en l'absence de la DPU, les journaux affichent le message SYS564 (`unable to perform system erase of DPU because there is no DPU available in the system`).
- Lorsque les cartes NVIDIA BF3 sont désactivées à partir de la configuration du BIOS, l'**état** est indiqué sur la page **Périphériques réseau**. Dans l'interface utilisateur de l'iDRAC, (**Système** > **Vue d'ensemble** > **Périphérique réseau** > **Récapitulatif**) s'affiche en vert.
- Lorsque les logements PCIe des cartes DPU NVIDIA BF3 indiquent **Lecteur de démarrage désactivé** dans la configuration du BIOS (**Paramètres du BIOS du système** > **Périphériques intégrés** > **Désactivation des logements)**, les journaux PR7 et PR8 s'affichent dans les journaux LC de l'iDRAC.
- L'inventaire matériel des périphériques s'affiche pour les cartes NVIDIA BF3 lorsque le logement PCIe indique **Lecteur de démarrage désactivé** dans la configuration du BIOS.
- Lorsque la carte RAN DPU Nokia est définie sur le mode d'économie d'énergie, les journaux LC critiques s'affichent.

Les DPU offrent les fonctionnalités suivantes :

- Vous pouvez configurer la synchronisation du démarrage de la DPU pour chaque logement compatible avec la DPU.
- Vous pouvez configurer la valeur du délai d'expiration du mode DPU OS Ready en minutes (de 0 à 30).

- Selon la configuration utilisateur, l'énumération PCIe du BIOS et le processus de démarrage du système d'exploitation/hyperviseur de l'hôte ne s'effectuent qu'une fois que chaque **DPU activée pour la synchronisation du démarrage** a signalé le système d'exploitation de la DPU comme prêt.
- Les autres fonctions PCIe exposées par le système d'exploitation de la DPU sont énumérées par le BIOS et consignées dans l'inventaire matériel de l'iDRAC.
- Le BIOS affiche divers messages en lien avec la DPU lors du POST :
  - **Détection des unités de traitement des données...** : lors de la détection des périphériques de DPU
  - **Détection des unités de traitement des données ... Terminée** : lorsque la découverte de la DPU est terminée.
  - **Initialisation de l'unité de traitement des données (Ne PAS redémarrer le système)** : à 0, 10, 20, 30, 40, 50, 60, 70, 80, 90 et 100 % de progression de la synchronisation du démarrage
  - **Initialisation de l'unité de traitement des données... Terminée** : lorsque la synchronisation du démarrage est arrivée à 100 % et lorsqu'elle a été réalisée avec succès.
- Les messages individuels et globaux DPU OS Ready sont consignés au LCL.

  REMARQUE : L'indicateur DPU OS Ready persiste lors des différents redémarrages de l'hôte et le message DPU OS Ready est consigné pour chaque redémarrage de l'hôte.

- En cas de tâche LC-SSM, le BIOS ignore le temps d'attente de la synchronisation du démarrage de la DPU.

Inventaire et surveillance des DPU

L'inventaire du système de l'iDRAC fournit la marque et le modèle de la DPU tout en surveillant l'intégrité des cœurs, des périphériques et du système d'exploitation installé de la DPU. Une opération `GET` permet de récupérer les informations d'inventaire. Cette action garantit qu'aucun périphérique non autorisé n'est installé de manière malveillante. L'opération GET vous permet de vérifier régulièrement l'intégrité de la DPU. Si le système est fonctionnel, il renvoie une réponse de charge utile et une mise à jour d'état à des fins de mises à jour d'intégrité.

Pour détecter toute installation malveillante ou accidentelle du système d'exploitation de la DPU, utilisez l'opération GET. Celle-ci vous permet de récupérer le nom du système d'exploitation de la DPU, le nom de son fournisseur, sa version et son état.

Vous pouvez afficher la DPU installée à partir de l'interface utilisateur de l'iDRAC en accédant à **Système** > **Inventaire** > **Inventaire du firmware**

Redfish

À l'aide de Redfish, vous pouvez définir une configuration de démarrage unique servant à démarrer la DPU avec la valeur configurée une fois au redémarrage. Lors du redémarrage suivant, le démarrage de la DPU suit l'ordre de démarrage configuré. Redfish permet également de mettre à jour les firmwares pour ARM-UEFI et BMC. Pour en savoir plus, voir developer.dell.com.

Console série

Pour accéder au contrôle de série à l'aide de RACADM, connectez-vous à l'interface SSH de l'iDRAC et exécutez la commande `Racadm> console dpu`

Arrêt coordonné

Le processus d'arrêt du système d'exploitation ESXi arrête en interne l'ESXio de la DPU afin de prévenir toute corruption des fichiers ESXio.

6

Gestion des plug-ins

Les plug-ins sont des composants logiciels qui étendent les fonctionnalités d'iDRAC. Les plug-ins sont fournis individuellement dans un package DUP. Les plug-ins ne sont pas supprimés lors du redémarrage, de la réinitialisation ou des cycles d'alimentation secteur de l'iDRAC. Ils sont supprimés via l'opération de nettoyage de l'iDRAC ou l'opération d'effacement LC. Vous pouvez activer ou désactiver les plug-ins.

Pour gérer les plug-ins à partir de l'interface utilisateur de l'iDRAC, accédez à **Paramètres de l'iDRAC** > **Paramètres** > **Plug-ins**.

REMARQUE : Vous devez disposer des droits de connexion, de contrôle et de configuration pour installer, mettre à jour et supprimer les plug-ins. Vous pouvez uniquement afficher les plug-ins installés avec des droits de connexion.

Sujets :

Installation d'un plug-in

Installez un plug-in si vous souhaitez étendre les fonctionnalités d'iDRAC. Certains plug-ins sont préinstallés dans l'iDRAC en usine Dell pour les serveurs PowerEdge à partir des 15e et 16e générations.

Lorsqu'une liste d'appareils non-standard, non-SDL (Non-Standard Device List) est installée, l'iDRAC ne détecte pas de plug-in SDK. Recherchez et installez manuellement le plug-in SDK. La mise à jour, la rétrogradation ou la restauration du firmware de l'iDRAC n'a pas d'impact sur la fonctionnalité des plug-ins.

1. Téléchargez le plug-in à partir de Dell.com.
2. Accédez à **Paramètres iDRAC** > **Paramètres** > **Plug-ins**.
3. Cliquez sur **Ajouter/Mettre à jour**.
4. Sélectionnez le **type d'emplacement**, cliquez sur **Choisir un fichier** et sélectionnez le fichier du plug-in.
5. Cliquez sur **Charger**.
   Si un plug-in est valide, un message de réussite s'affiche après l'installation du plug-in. Si le matériel n'est pas présent, un message LC s'affiche indiquant que le plug-in n'a pas démarré. Si le PIN n'est pas valide, un message d'erreur s'affiche.

Désinstallation d'un plug-in

1. Accédez à **Paramètres iDRAC** > **Paramètres** > **Plug-ins**.
2. Sélectionnez le plug-in et cliquez sur **Désinstaller**.
   Le plug-in sélectionné est désinstallé.

Redémarrer un plug-in

Vous pouvez redémarrer un plug-in installé dans l'iDRAC.

1. Accédez à **Paramètres iDRAC** > **Paramètres** > **Plug-ins**.
2. Cliquez sur **Redémarrer**.

Activer ou désactiver un plug-in

Vous pouvez activer ou désactiver un plug-in.

1. Accédez à **Paramètres iDRAC** > **Paramètres** > **Plug-ins**.
2. Sélectionnez le plug-in et cliquez sur **Activer** ou sur **Désactiver**.

Afficher les détails du plug-in

Vous pouvez afficher les détails des plug-ins installés.

1. Accédez à **Paramètres iDRAC** > **Paramètres** > **Plug-ins**.
2. Sélectionnez le plug-in et cliquez sur **Détails**.
   Les informations détaillées concernant le plug-in s'affichent.

7

Configuration de l'iDRAC

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

Avant de configurer l'iDRAC, assurez-vous que les paramètres réseau de l'iDRAC et un navigateur pris en charge sont configurés, et que les licences requises sont mises à jour. Pour plus d'informations sur les fonctionnalités sous licence de l'iDRAC, voir Licences iDRAC.

Configurez iDRAC en utilisant :

- Interface web iDRAC
- RACADM
- IPMITool (voir le **Guide de l'utilisateur de Baseboard Management Controller Management**).

REMARQUE : Lorsqu'un travail ou une tâche est en cours, ne redémarrez pas ou n'arrêtez le système ou n'effectuez pas de cycle d'alimentation CA de l'hôte ou de l'iDRAC via n'importe quel mode (manuel ou en appuyant sur « Ctrl+Alt+Suppr » ou via les options fournies dans les interfaces de l'iDRAC). Le système (hôte et iDRAC) doit toujours être redémarré ou arrêté normalement lorsqu'aucune tâche n'est en cours d'exécution dans l'iDRAC ou l'hôte. Un arrêt anormal ou une opération interrompue peut avoir des conséquences imprévisibles, telles que la corruption du firmware, générer des fichiers noyaux, des RSOD, des YSOD, des événements d'erreur dans LCL, etc.

Pour configurer iDRAC :

1. Connectez-vous à iDRAC.
2. Modifiez les paramètres réseau, si nécessaire.

   REMARQUE : Si vous avez défini les paramètres réseau iDRAC en utilisant l'utilitaire de Configuration d'iDRAC pendant la définition de l'adresse IP iDRAC, ignorez cette étape.

3. Définissez les interfaces d'accès à iDRAC.
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 iDRAC :
   - IPMI ou RAC série
   - IPMI série sur LAN
   - IPMI sur le LAN
   - SSH
8. Obtenez les certificats nécessaires.
9. Ajoutez et configurez des utilisateurs iDRAC 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. Définissez le premier périphériques de démarrage, si nécessaire.
15. Définissez la connexion directe entre le SE et iDRAC, le cas échéant.

Sujets :

- Définition du premier périphérique de démarrage
- Activation ou désactivation de la connexion directe entre le SE et l'iDRAC
- Obtention de certificats
- Configuration de plusieurs iDRAC à l'aide de RACADM
- Désactivation de l'accès pour modifier les paramètres de configuration iDRAC sur un système hôte

Affichage des informations iDRAC

Vous pouvez afficher les propriétés de base d'iDRAC.

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

Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Présentation** pour afficher les informations suivantes relatives à l'iDRAC. Pour plus d'informations sur les propriétés, voir l'**Aide en ligne de l'iDRAC**.

Détails d'iDRAC

- Type d'appareil
- Version du matériel
- Version du firmware
- Mise à jour de firmware
- Heure RAC
- Version IPMI
- Nombre de sessions possibles
- Nombre de sessions actives en cours
- Version IPMI

iDRAC Service Module

- État

Vue de connexion

- État
- ID de connexion de commutateur
- ID de connexion du port du commutateur

Paramètres réseau actuels

- Adresse MAC d'iDRAC
- Interface de carte réseau active
- Nom de domaine DNS

Paramètre IPv4 actuel

- IPv4 activé
- DHCP
- Adresse IP actuelle
- Masque de sous-réseau actuel
- Passerelle actuelle
- Utilisation de DHCP pour obtenir l'adresse du serveur DNS
- Serveur DNS préféré actuel
- Autre serveur DNS actuel

Paramètres IPv6 actuels

- Activation IPv6
- Configuration automatique
- Adresse IP actuelle
- Passerelle IP actuelle
- Adresse locale de liaison
- Utiliser DHCPv6 pour obtenir des DNS
- Serveur DNS préféré actuel

- Autre serveur DNS actuel

Affichage des informations iDRAC à l'aide de RACADM

Pour afficher les informations iDRAC à l'aide de RACADM, voir les détails sur la sous-commande `getsysinfo` ou `get` fournis dans le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Modification des paramètres réseau

Après avoir configuré les paramètres réseau de l'iDRAC à l'aide de l'utilitaire de configuration de l'iDRAC, vous pouvez également modifier les paramètres via l'interface Web iDRAC, RACADM, Lifecycle Controller et Server Administrator (après le démarrage du système d'exploitation). Pour plus d'informations sur les outils et les paramètres de privilèges, reportez-vous aux guides de l'utilisateur correspondants.

Pour pouvoir modifier les paramètres réseau à l'aide de l'interface Web d'iDRAC ou RACADM, vous devez disposer des privilèges de **Configuration**.

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

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

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

```
racadm get iDRAC.Nic
```

Pour utiliser DHCP afin d'obtenir une adresse IP, utilisez la commande suivante pour écrire l'objet `DHCPEnable` et activer cette fonctionnalité.

```
racadm set iDRAC.IPv4.DHCPEnable 1
```

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

```
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 `iDRAC.Nic.Enable` est définie sur **0**, le LAN de l'iDRAC est désactivé, même si DHCP est activé.

Modification des paramètres réseau à l'aide de l'interface Web

Pour modifier les paramètres réseau iDRAC :

1. Dans l'interface Web d'iDRAC, accédez à **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Paramètres 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 dédiée automatiquement** sous **Paramètres réseau**, lorsque les cartes réseau de l'iDRAC sont sélectionnées en tant que LOM partagé (1, 2, 3, ou 4) et 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 ; le temps d'arrêt du passage de Dédié à Partagé est de 30 secondes. Vous pouvez configurer la valeur d'expiration à l'aide de RACADM.

Pour plus d'informations sur les champs, voir l'**aide en ligne d'iDRAC**.

REMARQUE : Si l'iDRAC utilise DHCP et dispose d'un contrat de location longue durée pour son adresse IP, ce contrat DHCP est transmis vers le pool d'adresses de serveur DHCP lorsque la carte NIC, l'IPv4 ou le DHCP est désactivé.

Sélection des suites de chiffrement

La sélection des suites de chiffrement permet de limiter les chiffrements dans l'iDRAC ou les communications client et de déterminer le niveau de sécurité de la connexion. Elle fournit un autre niveau de filtrage de la suite de chiffrement TLS effective utilisée. Ces paramètres peuvent être configurés via l'interface Web de l'iDRAC et les interfaces de ligne de commande RACADM.

Configuration de la sélection des suites de chiffrement à l'aide de RACADM

Pour configurer la sélection des suites de chiffrement à l'aide de RACADM, utilisez l'une des commandes suivantes :

- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-GCM-SHA384`
- `racadm set idraC.webServer.customCipherString ALL:-DHE-RSA-CAMELLIA256-SHA`
- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-SHA256:+AES256-GCM-SHA384:-DHE-RSA-CAMELLIA256-SHA`

Pour plus d'informations sur ces objets, voir le **Guide de référence de l'interface de ligne de commande RACADM d'iDRAC**, disponible sur la page Manuels iDRAC.

Configuration de la sélection des suites de chiffrement à l'aide de l'interface Web de l'iDRAC

PRÉCAUTION : L'utilisation de la commande de chiffrement OpenSSL pour l'analyse de chaînes avec une syntaxe invalide peut conduire à des erreurs inattendues.

REMARQUE : Il s'agit d'une option de sécurité avancée. Avant de configurer cette option, vous devez posséder une connaissance approfondie des éléments suivants :

- La syntaxe de la chaîne chiffrée OpenSSL et son utilisation.
- Les outils et procédures nécessaires pour valider la configuration de la suite de chiffrement qui en résulte, afin de vous assurer que les résultats correspondent aux attentes et aux exigences.

REMARQUE : Avant de configurer les paramètres avancés des suites de chiffrement TLS, assurez-vous d'utiliser un navigateur web pris en charge.

REMARQUE : Quelle que soit la version TLS configurée dans l'iDRAC, le navigateur Firefox de RHEL vous permet de lancer l'interface graphique de l'iDRAC.

REMARQUE : Pour obtenir la liste des chiffrements pour un port spécifique, exécutez l'outil nmap.

Pour ajouter des chaînes chiffrées personnalisées :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Services** > **Serveur Web**.
2. Cliquez sur **Définir une chaîne chiffrée** dans l'option **Chaîne chiffrée personnalisée**.
   La page **Définir une chaîne chiffrée personnalisée** s'affiche.
3. Dans le champ **Chaîne chiffrée personnalisée**, saisissez une chaîne valide et sélectionnez **Définir une chaîne chiffrée**.

   REMARQUE :
   - Pour plus d'informations sur les chaînes de chiffrement, voir la page OpenSSL.

- TLS 1.3 n'est pas pris en charge.

4. Cliquez sur **Appliquer**.
   La définition de la chaîne chiffrée personnalisée met fin à la session iDRAC actuelle. Attendez quelques minutes avant d'ouvrir une nouvelle session iDRAC.

Mode FIPS

FIPS est une norme de sécurité des ordinateurs que les agences et les sous-traitants du gouvernement des États-Unis doivent utiliser. L'iDRAC prend en charge l'activation du mode FIPS.

iDRAC sera dans le futur officiellement certifié comme prenant en charge le mode FIPS.

Différence entre le mode prise en charge de FIPS et validé FIPS

Un logiciel validé à l'issue du programme de validation des modules cryptographiques est dit « validé par FIPS ». En raison du temps nécessaire à la validation FIPS, toutes les versions de l'iDRAC ne sont pas validées. Pour plus d'informations sur l'état le plus récent de la validation FIPS pour l'iDRAC, consultez la page Cryptographic Module Validation Program sur le site Web du NIST.

Désactivation du mode FIPS

Pour désactiver le mode FIPS, vous devez réinitialiser iDRAC pour restaurer ses paramètres d'usine par défaut.

Activation du mode FIPS

PRÉCAUTION : Si vous activez le mode FIPS, la configuration par défaut de l'iDRAC sera rétablie. Si vous souhaitez restaurer les paramètres, sauvegardez le profil de configuration de serveur (SCP) avant d'activer le mode FIPS, et restaurez le SCP après redémarrage de l'iDRAC.

Configuration des services

Vous pouvez configurer et activer les services suivants sur iDRAC :

Configuration locale	Désactivez l'accès à la configuration iDRAC (depuis le système hôte) à l'aide de l'interface locale RACADM et l'utilitaire de configuration iDRAC.
Serveur Web	Activer l'accès à l'interface Web d'iDRAC. Si vous désactivez l'interface Web, l'interface RACADM distante est également désactivée. Utilisez la RACADM locale pour réactiver le serveur Web et la RACADM distante.
Configuration de SEKM	Active la fonctionnalité de gestion des clés d'entreprise sécurisées sur l'iDRAC à l'aide d'une architecture de serveur client.
SSH	Accédez à iDRAC via le firmware de RACADM.
Interface RACADM distante	Accédez à distance à iDRAC.
Agent SNMP	Active la prise en charge des requêtes SNMP (opérations GET, GETNEXT et GETBULK) dans iDRAC.
Agent de récupération de système automatique	Activez l'affichage de l'écran du dernier blocage du système.
Redfish	Active la prise en charge de l'API RESTful Redfish.
Serveur VNC	Activez le serveur VNC avec ou sans chiffrement SSL.

Configuration des services à l'aide de RACADM

Pour activer et configurer les services à l'aide de RACADM, utilisez la commande `set` avec les objets des groupes suivants :

- iDRAC.LocalSecurity
- iDRAC.LocalSecurity
- iDRAC.SSH
- iDRAC.Webserver
- iDRAC.Racadm
- iDRAC.SNMP

Pour plus d'informations sur ces objets, voir Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Configuration des services en utilisant l'interface web

Pour configurer les services en utilisant l'interface web d'iDRAC :

1. Dans l'interface Web d'iDRAC, accédez à **Paramètres iDRAC** > **Services**.
   La page **Services** s'affiche.
2. Entrez les informations requises, puis cliquez sur **Appliquer**.
   Pour plus d'informations sur les paramètres, voir l'**Aide en ligne d'iDRAC**.

   REMARQUE : Ne cochez pas la case **Empêcher cette page de générer des boîtes de dialogue supplémentaires**. La sélection de cette option empêche en effet la configuration des services.

   Vous pouvez configurer **SEKM** depuis la page Paramètres iDRAC. Cliquez sur **Paramètres iDRAC** > **Services** > **Configuration SEKM** .

   REMARQUE : Pour une procédure étape par étape détaillée pour configurer SEKM, reportez-vous à **l'aide en ligne de l'iDRAC**.

   REMARQUE : Lorsque le mode **Sécurité (chiffrement)** est modifié de **Aucun** à **SEKM**, la tâche en temps réel n'est pas disponible. Mais elle sera ajoutée à la liste de tâches échelonnée. Cependant, la tâche en temps réel est réussie si le mode est modifié de **SEKM** à **Aucun**.

   Vérifiez les éléments suivants lors de la modification de la valeur du champ **Nom d'utilisateur** dans la section Certificat client sur le serveur KeySecure (par ex : la modification de la valeur de **Nom de domaine (CN)** à **ID utilisateur (UID)**)

   a. Lorsque vous utilisez un compte existant :
      - Vérifiez dans le certificat SSL de l'iDRAC que, à la place du champ **Nom commun**, le champ **Nom d'utilisateur** correspond maintenant au nom d'utilisateur existant sur le KMS. Si cela n'est pas le cas, vous aurez alors besoin de définir le champ Nom d'utilisateur et de régénérer le certificat SSL à nouveau, le faire signer sur KMS et le télécharger à nouveau vers l'iDRAC.

   b. Lors de l'utilisation d'un nouveau compte d'utilisateur :
      - Assurez-vous que la chaîne **Nom d'utilisateur** correspond au champ du nom d'utilisateur dans le certificat SSL de l'iDRAC.
      - Si elle ne correspond pas, vous devrez reconfigurer les attributs Nom d'utilisateur et Mot de passe de KMS iDRAC .
      - Une fois qu'il est établi que le certificat contient le nom d'utilisateur, le seul changement qui doit être fait consiste à modifier la propriété de la clé de l'ancien utilisateur vers le nouvel utilisateur nouvellement créé pour correspondre au nom d'utilisateur KMS.

   Lors de l'utilisation de Vormetric Data Security Manager comme KMS, assurez-vous que le champ Nom commun (CN) dans le certificat SSL iDRAC correspond au nom de l'hôte ajouté à Vormetric Data Security Manager. Dans le cas contraire, le certificat ne peut pas être importé avec succès.

   REMARQUE :
   - L'option **Réaffectation** sera désactivée lorsque `racadm sekm getstatus` signale un **Échec**.
   - SEKM ne prend en charge **Nom commun**, **ID utilisateur**, ou **Unité organisationnelle** pour le champ **Nom d'utilisateur** sous le Certificat de client.
   - Si vous utilisez une autorité de certification tiers pour signer la CSR iDRAC, assurez-vous qu'elle prend en charge la valeur **UID** pour le champ **Nom d'utilisateur** dans le Certificat de client. Si elle n'est pas prise en charge, utilisez **Nom commun** comme la valeur du champ **Nom d'utilisateur**.
   - Si vous utilisez des champs Nom d'utilisateur et Mot de passe, assurez-vous que le serveur KMS prend en charge ces attributs.

REMARQUE : Dans le cadre d'un serveur de gestion de clés KeySecure, lors de la création d'une demande de certificat SSL, vous devez indiquer au moins l'une des adresses IP ou le nom DNS du serveur de gestion des clés dans le champ **Autre nom de l'objet**. Assurez-vous que l'adresse IP est au format IP:xxx.xxx.xxx.xxx.xxx. Xxx.

Fonctionnalités de la solution iLKM

La solution de gestion des clés locales de l'iDRAC (iLKM) est une solution de sécurité similaire à la solution de gestion des clés d'entreprise sécurisées (SEKM). Elle est idéale pour les utilisateurs qui ne prévoient pas d'utiliser SEKM, mais qui souhaitent sécuriser les appareils à l'aide de l'iDRAC. Toutefois, les clients pourront migrer vers SEKM ultérieurement. Pour plus d'informations, consultez le livre blanc Activer iLKM sur les serveurs Dell PowerEdge

.

Lors de l'utilisation d'iLKM, l'iDRAC agit en tant que gestionnaire de clés et génère des clés d'authentification utilisées pour sécuriser les périphériques de stockage. Pour utiliser iLKM en tant que système de gestion des clés, accédez à **Paramètres iDRAC** > **Services** > **Gestion des clés de l'iDRAC** et sélectionnez iLKM dans le menu déroulant.

REMARQUE : iLKM nécessite une combinaison de la licence SEKM et de la licence iDRAC Enterprise, ou de la licence SEKM et de la licence iDRAC Datacenter.

Spécifiez une phrase secrète et un ID de clé pour activer iLKM. La phrase secrète et l'ID de clé doivent comporter 255 caractères maximum.

REMARQUE :

- Il est possible d'afficher et de configurer iLKM via l'interface utilisateur de l'iDRAC ainsi que les interfaces RACADM et Redfish.
- Vous pouvez activer ou désactiver la sécurité sur les disques SED NVMe pris en charge lorsque l'iDRAC est en mode de sécurité iLKM.
- Vous ne pouvez pas activer, désactiver ni recréer la clé iLKM en mode System Lockdown.
- Actuellement, iLKM prend uniquement en charge les disques SED NVMe connectés directement, compatibles avec le protocole TCG Opal 2.0 et les versions ultérieures.
- iLKM fournit une option de recréation de clé, dans laquelle vous devez fournir la phrase secrète et l'ID de clé pour l'authentification.

Sécuriser automatiquement les disques pris en charge

- Option permettant de demander à l'iDRAC de sécuriser automatiquement les disques NVMe SED et SAS SED non connectés à PERC derrière un adaptateur HBA SAS sécurisé. Les disques sont automatiquement sécurisés lors d'un redémarrage de l'hôte ou d'un enfichage à chaud de disque.
- L'option n'active pas automatiquement la sécurité sur les contrôleurs tels que PERC et HBA SAS.
- Cette option est activée par défaut : vous pouvez la désactiver à l'aide de la commande RACADM.
- Désactivez cette option avant la réaffectation d'un disque à l'aide de l'option d'effacement cryptographique (ou de l'option Rétablir le PSID) s'il n'est plus nécessaire de sécuriser le disque via l'iDRAC.

REMARQUE : Les disques NVMe à connexion directe peuvent être des disques compatibles ou non avec le chiffrement. Les journaux SEKM 044 sont générés pour les disques non compatibles avec le chiffrement, car l'état du plug-in est vérifié pour les deux disques NVMe à connexion directe pendant l'opération de sécurisation automatique.

REMARQUE : Les opérations de rétablissement du PSID ne sont possibles que sur les disques verrouillés ou étrangers. Il est impossible d'effectuer ces opérations sur les disques connectés au contrôleur PERC.

REMARQUE : N'effectuez pas de cycle d'alimentation sur le système hôte immédiatement après l'activation de l'option **Sécuriser automatiquement les disques pris en charge**. Cela risque d'interrompre l'activation de la sécurité sur les disques et de placer les disques dans un état de sécurité non défini.

Transition de la solution iLKM vers la solution SEKM

Vous devez fournir la phrase secrète de la solution iLKM pour authentifier la transition, ainsi que les détails de configuration SEKM. Si l'authentification réussit, SEKM est activé sur l'iDRAC et l'ID de clé iLKM précédent est supprimé. Pour passer de la solution iLKM à la solution SEKM, procédez comme suit :

1. Configurez le certificat CSA.
2. Configurez les paramètres SEKM.
3. Effectuez la transition de la solution iLKM vers la solution SEKM.

Fonctionnalités SEKM

Vous trouverez ci-dessous les fonctionnalités SEKM disponibles dans l'iDRAC :

1. **Stratégie de purge des clés SEKM** : l'iDRAC fournit un paramètre de stratégie qui vous permet de configurer l'iDRAC afin de purger les anciennes clés inutilisées sur le serveur de gestion de clés (KMS) lors de l'exécution de l'opération Recréer la clé. Vous pouvez définir l'attribut de lecture-écriture KMSKeyPurgePolicy de l'iDRAC sur l'une des valeurs suivantes :
   - Conserver toutes les clés : il s'agit du paramètre par défaut et du comportement existant où l'iDRAC laisse toutes les clés sur le KMS intactes lors de l'exécution de l'opération Recréer la clé.
   - Conserver les clés N et N-1 : l'iDRAC supprime toutes les clés du KMS, à l'exception de la clé actuelle (N) et de la clé précédente (N-1) lors de l'exécution de l'opération Recréer la clé.
2. **Purge des clés KMS sur SEKM désactivé** : dans le cadre de la solution Secure Enterprise Key Manager (SEKM), l'iDRAC vous permet de désactiver SEKM sur l'iDRAC. Une fois SEKM désactivé, les clés générées par l'iDRAC au KMS sont inutilisées et restent au KMS. Cette fonctionnalité permet à l'iDRAC de supprimer ces clés lorsque SEKM est désactivé. L'iDRAC fournit une nouvelle option « -purgeKMSKeys » à la commande existante « racadm sekm disable », ce qui vous permet de purger les clés au KMS lorsque SEKM est désactivé sur l'iDRAC.

   REMARQUE : Si SEKM est déjà désactivé et que vous souhaitez purger les anciennes clés, vous devez réactiver SEKM, puis désactiver le passage dans l'option -purgeKMSKeys.

3. **Stratégie de création de clé** : dans le cadre de cette version, l'iDRAC a été préconfiguré avec une stratégie de création de clé. L'attribut KeyCreationPolicy est en lecture seule et défini sur la valeur « Key per iDRAC ».
   - L'attribut iDRAC iDRAC.SEKM.KeyIdentifierN en lecture seule indique l'ID de la clé créée par le KMS.

     ```
     racadm get iDRAC.SEKM.KeyIdentifierN
     ```

   - L'attribut iDRAC iDRAC.SEKM.KeyIdentifierNMinusOne en lecture seule indique l'ID de clé précédent après avoir effectué une opération Recréer la clé.

     ```
     racadm get iDRAC.SEKM.KeyIdentifierNMinusOne
     ```

4. **Recréer la clé SEKM** : l'iDRAC fournit les deux options suivantes à partir de l'interface utilisateur pour recréer la clé de votre solution SEKM, Recréer la clé iDRAC ou PERC. Il est recommandé de recréer la clé de l'iDRAC, car cela permet de recréer les clés de tous les appareils compatibles SEKM Secure.
   - **Recréer la clé SEKM iDRAC [Recréer la clé sur iDRAC.Embedded.1 FQDD]** : lors de l'exécution de `racadm sekm rekey iDRAC.Embedded.1`, les clés de tous les appareils compatibles SEKM Secure sont recréées à l'aide d'une nouvelle clé de KMS. Il s'agit d'une clé commune à tous les appareils compatibles SEKM. L'opération Recréer la clé de l'iDRAC peut également être effectuée à partir de l'interface utilisateur de l'iDRAC : **Paramètres iDRAC** > **Services** > **Configuration SEKM** > **Recréer la clé**. Après avoir exécuté cette opération, les modifications apportées à la clé peuvent être validées en lisant les attributs KeyIdentifierN et KeyIdentifierNMinusOne.
   - **Recréer la clé SEKM PERC (Recréer la clé sur le FQDD du contrôleur [Exemple de RAID.Slot.1-1])** : lors de l'exécution de `racadm sekm rekey <controller FQDD>`, le contrôleur SEKM correspondant est renouvelé avec la clé commune de l'iDRAC actuellement active créée à partir de KMS. L'opération Recréer la clé du contrôleur de stockage peut également être exécutée à partir de l'interface utilisateur de l'iDRAC comme suit : **Stockage** > **Contrôleurs** > **<FQDD du contrôleur>** > **Actions** > **Modifier** > **Sécurité** > **Sécurité (Chiffrement)** > **Recréer la clé**.

     REMARQUE : lorsque vous recréez la clé sur PERC alors que les clés du contrôleur et de l'iDRAC sont synchronisées, vous pouvez rencontrer un **échec de tâche de configuration**, ou la tâche de configuration peut réussir, mais la clé rester inchangée lorsque vous exécutez la tâche. Vous pouvez utiliser l'option Recréer la clé de l'iDRAC pour résoudre ce problème.

5. **Recréer la clé SEKM uniquement à partir de Redfish** : les deux options de recréation de clé SEKM suivantes sont prises en charge par Redfish :
   - **Planifier la recréation de clé SEKM iDRAC** : envoie une nouvelle demande de génération de clé à partir de l'iDRAC pour modifier automatiquement les clés SEKM selon un intervalle de récurrence configuré par l'utilisateur.
   - **Synchronisation périodique d'iDRAC SEKM avec Key Management Server (KMS)** : active la modification automatique des clés SEKM en fonction de l'intervalle de récurrence configuré sur le serveur KMS. L'iDRAC interroge toute nouvelle clé générée par le serveur KMS.

Pour obtenir des informations détaillées sur toutes les fonctionnalités SEKM prises en charge et sur le workflow de déploiement, voir le livre blanc Activation d'OpenManage Secure Enterprise Key Manager (SEKM) sur des serveurs Dell PowerEdge.

REMARQUE : lorsque SEKM est activé sur PERC, un journal CTL136 est généré. Cependant, dans PERC 12, lors de la recréation de la clé, le journal CTL136 n'est pas généré. Cela est dû au fait que le contrôleur ne crée pas de demande de clé, car les clés sont fournies dans le cadre de la commande de recréation de clé.

Activation ou désactivation de la redirection HTTPS

Si vous souhaitez désactiver la redirection automatique de HTTP vers HTTPS en raison d'un problème d'avertissement avec le certificat de l'iDRAC par défaut ou en tant que paramètre temporaire à des fins de débogage, vous pouvez configurer l'iDRAC de sorte à désactiver la redirection du port http (par défaut, 80) vers le port https (par défaut, 443). Par défaut, il est activé. Vous devez vous déconnecter et vous connecter à l'iDRAC pour que ce paramètre prenne effet. Si vous désactivez cette fonctionnalité, un message d'avertissement s'affiche.

Vous devez disposer du privilège de configuration de l'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 la redirection de HTTP vers HTTPS :

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

Pour activer la redirection de HTTP vers HTTPS :

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

Pour afficher l'état de la redirection de HTTP vers 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 des ordinateurs de bureau et des appareils 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 mesures correctives 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. Vous pouvez configurer ces paramètres dans l'interface Web de l'iDRAC ou RACADM.

REMARQUE : La fonction VNC est sous licence et est disponible sous la licence iDRAC Enterprise ou Datacenter.

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

Deux sessions client VNC peuvent être activées simultanément. La seconde session est en mode En lecture seule.

Si une session VNC est active, vous pouvez uniquement lancer le support virtuel à l'aide de l'option Lancer la console virtuelle et non à l'aide du visualiseur de console virtuelle.

Si le chiffrement vidéo est désactivé, le client VNC établit des liaisons RFB directement et les liaisons SSL sont inutiles. Pendant l'établissement d'une liaison 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 d'une liaison, le serveur VNC désactive la console virtuelle et seul le support virtuel est autorisé. Une fois la session VNC terminée, le serveur VNC restaure l'état d'origine de la console virtuelle (activée ou désactivée).

REMARQUE :

- Lorsque vous lancez une session VNC, si vous obtenez une erreur de protocole RFB, définissez les paramètres du client VNC sur haute qualité, puis relancez la session.
- Lorsque la carte réseau de l'iDRAC est en mode partagé et le système hôte est redémarré, la connexion réseau est interrompue pendant quelques secondes. Pendant ce temps, si vous effectuez une action dans le client VNC actif, la session VNC peut fermer. Vous devez attendre le délai d'expiration (la valeur configurée des paramètres du serveur VNC dans la page **Services** de l'interface Web de l'iDRAC) puis rétablir la connexion VNC.
- Si la fenêtre du client VNC est réduite pendant plus de 60 secondes, elle se ferme. Vous devez ouvrir une nouvelle session VNC. Si vous agrandissez la fenêtre du client VNC dans les 60 secondes, vous pouvez continuer à l'utiliser.

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 de l'iDRAC, accédez à **Configuration** > **Console virtuelle**.
   La page **Console virtuelle** 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 d'iDRAC**.
3. Cliquez sur **Appliquer**.
   Le serveur VNC est configuré.

Configuration du serveur VNC à l'aide de RACADM

Pour configurer le serveur VNC, utilisez la commande `set` avec les objets de `VNCserver`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Configuration de VNC Viewer avec cryptage SSL

Lors de la configuration des paramètres du serveur VNC dans l'iDRAC, si l'option **Chiffrement SSL** a été activé, l'application de tunnel SSL doit être utilisée avec le VNC Viewer pour établir la connexion SSL chiffrée avec le serveur VNC d'iDRAC.

REMARQUE : La prise en charge du cryptage SSL n'est pas intégrée à la plupart des clients VNC.

Pour configurer l'application de tunnel SSL :

1. Configurez le tunnel SSL pour accepter la connexion sur `<localhost>:<localport number>`. Par exemple, 127.0.0.1:5930.
2. Configurez le tunnel SSL pour vous connecter à `<iDRAC IP address>:<VNC server port Number>`. Par exemple, 192.168.0.120:5901.
3. Démarrez l'application de tunnel.
   Pour établir une connexion avec le serveur VNC d'iDRAC sur le canal crypté SSL, connectez le VNC Viewer à l'hôte local (lien adresse IP locale) et le numéro de port local (127.0.0.1 : <numéro de port local>).

Configuration de VNC Viewer sans cryptage SSL

En règle générale, toutes les instances de VNC Viewer conformes RFB (Remote Frame Buffer) se connectent au serveur VNC à l'aide de l'adresse IP et du numéro de port de l'iDRAC configurés pour le serveur VNC. Si l'option de chiffrement SSL est désactivée lors de la configuration des paramètres du serveur VNC dans l'iDRAC, procédez comme suit pour vous connecter à VNC Viewer :

Dans la boîte de dialogue **VNC Viewer**, entrez l'adresse IP d'iDRAC et le numéro de port VNC dans le champ **Serveur VNC**.

Le format est le suivant : `<iDRAC IP address:VNC port number>`

Par exemple, si l'adresse IP de l'iDRAC est 192.168.0.120 et que le numéro de port VNC est 5901, saisissez `192.168.0.120:5901`.

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. Après avoir mis à jour les paramètres du serveur NTP, déconnectez-vous de toutes les sessions en cours, puis connectez-vous à l'iDRAC.

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

Lorsque vous activez ou désactivez les paramètres du serveur NTP, déconnectez-vous de toutes les sessions en cours, puis connectez-vous à l'iDRAC.

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

1. Accédez à **Paramètres iDRAC** > **Paramètres** > **Fuseau horaire et paramètres de NTP**.
   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 d'iDRAC**.

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

Pour configurer le fuseau horaire et le NTP, utilisez la commande `set` avec les objets du groupe `iDRAC.Time` et `iDRAC.NTPConfigGroup`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

REMARQUE : L'iDRAC synchronise l'heure avec l'hôte (heure locale). Par conséquent, il est recommandé de configurer à la fois l'iDRAC et l'hôte avec le même fuseau horaire afin que la synchronisation de l'heure soit correcte. Si vous souhaitez modifier un fuseau horaire, vous devez le modifier sur l'hôte et l'iDRAC. L'hôte doit être ensuite redémarré.

Définition du premier périphérique de démarrage

Vous pouvez définir un périphérique de démarrage initial pour le prochain démarrage uniquement ou pour tous les redémarrages suivants. Si vous définissez un périphérique à utiliser lors de tous les démarrages suivants, il reste le périphérique de démarrage initial dans l'ordre de démarrage des périphériques configuré dans le BIOS jusqu'à ce qu'il soit modifié dans l'interface Web d'iDRAC ou la séquence de démarrage du BIOS.

Vous pouvez définir comme premier périphérique de démarrage l'un des dispositifs suivants :

- Démarrage normal
- PXE
- configuration du BIOS
- Support amovible disquette/principal local
- CD/DVD local
- Disque dur
- Disquette virtuelle
- CD/DVD/ISO virtuel
- Lifecycle Controller
- Gestionnaire d'amorçage du BIOS
- Chemin d'accès au périphérique UEFI
- UEFI HTTP (Amorçage hérité/UEFI)
- Fichier réseau virtuel 1
- Fichier réseau virtuel 2

REMARQUE :

- Configuration du BIOS (F2), Lifecycle Controller (F10), et Gestionnaire d'amorçage du BIOS (F11) ne peuvent pas être définis comme des périphériques d'amorçage permanents.
- Les paramètres du premier périphérique de démarrage dans l'interface web d'iDRAC remplacent les paramètres de démarrage du BIOS du système.

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

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

1. Accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Premier périphérique de démarrage**.
   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 à partir du périphérique sélectionné une seule fois lors du prochain démarrage, sélectionnez **Démarrer une fois**. Par la suite, le système démarre à partir du premier périphérique de démarrage dans l'ordre de démarrage du BIOS.

   Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

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

- Pour définir le premier périphérique de démarrage, utilisez l'objet `iDRAC.ServerBoot.FirstBootDevice`.
- Pour activer l'option de démarrage ponctuel pour un périphérique, utilisez l'objet `iDRAC.ServerBoot.BootOnce`.

Pour plus d'informations sur ces objets, voir Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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

Vous pouvez sélectionner l'appareil à partir duquel effectuer le démarrage comme serveur qui figure dans la visionneuse de la console virtuelle avant que le serveur exécute la séquence de démarrage. Le démarrage unique (Boot-once) est pris en charge par tous les appareils répertoriés dans la 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 ou désactivation de la connexion directe entre le SE et l'iDRAC

Dans les serveurs équipés d'une carte OCP (Open Compute Project) ou LAN intégrée sur la carte mère (LOM), vous pouvez activer la fonction Pass-through (Connexion directe) entre le système d'exploitation et iDRAC. Cette fonctionnalité fournit une communication intrabande bidirectionnelle à haute vitesse entre le contrôleur iDRAC et le système d'exploitation hôte au moyen d'un LOM partagé, d'une carte réseau dédiée ou via la carte réseau USB. Cette fonctionnalité est disponible pour la licence iDRAC Enterprise ou Datacenter.

REMARQUE : L'iDRAC Service Module (iSM) offre davantage de fonctionnalités pour gérer iDRAC via le système d'exploitation. Pour plus d'informations, voir le guide de l'utilisateur de l'iDRAC Service Module disponible sur la page iDRAC Service Module.

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.

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 :

- Interface web iDRAC
- RACADM (environnement post-système d'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 configurez le serveur en utilisant un profil de configuration de serveur via RACADM ou Redfish et si vous modifiez les paramètres réseau, vous devez patienter 15 secondes pour activer la fonction de connexion directe entre le système d'exploitation et iDRAC ou pour définir l'adresse IP de l'hôte du système d'exploitation.

Avant d'activer la fonction de connexion directe entre le SE et l'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 iDRAC se trouvent dans le même sous-réseau et le même VLAN.
- L'adresse IP du système d'exploitation hôte est configurée.
- Une carte prenant en charge la fonctionnalité d'intercommunication du SE vers 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 plusieurs LOM sont actifs, saisissez l'adresse IP du premier LOM.

Si la connexion directe entre le SE et l'iDRAC ne fonctionne pas après son activation, vérifiez les éléments suivants :

- Le câble de carte réseau dédié de l'iDRAC est bien connecté.
- Au moins un LOM est actif.

REMARQUE : Utilisez l'adresse IP par défaut. Assurez-vous que l'adresse IP de l'interface NIC USB ne se trouve pas dans le même sous-réseau que les adresses IP du système d'exploitation hôte ou de l'iDRAC. Si cette adresse IP est en conflit avec une adresse IP d'autres interfaces du système hôte ou du réseau local, vous devez la modifier.

REMARQUE : Si vous lancez l'iDRAC Service Module alors que la carte réseau USB est désactivée, l'iDRAC Service Module remplace l'adresse IP de la carte réseau USB par 169.254.0.1.

REMARQUE : N'utilisez pas les adresses IP 169.254.0.3 et 169.254.0.4. Ces adresses IP sont réservées au port de la carte réseau USB sur le panneau avant en cas d'utilisation d'un câble USB Type-C.

REMARQUE : Le contrôleur iDRAC peut ne pas être accessible à partir du serveur hôte à l'aide de LOM-Passthrough lorsque l'association de cartes réseau est activée. Le contrôleur iDRAC est alors accessible via le système d'exploitation du serveur hôte à l'aide de la carte réseau USB de l'iDRAC ou via le réseau externe, via la carte réseau dédiée de l'iDRAC.

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

Pour obtenir la liste des systèmes d'exploitation pris en charge pour la carte réseau USB, voir la note de mise à jour correspondante dans Versions et notes de mise à jour de l'iDRAC.

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

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

REMARQUE :

- Si vous désactivez la carte réseau USB sur l'iDRAC alors que l'iSM est en cours d'exécution dans le système d'exploitation, l'état du module de service iSM passe à sur « En cours d'exécution (fonctionnalités limitées) ».
- Si vous installez l'iSM dans le système d'exploitation alors que la carte réseau USB est désactivée dans l'iDRAC, l'iSM active automatiquement la carte réseau USB dans l'iDRAC pour terminer l'installation. Si nécessaire, désactivez la carte réseau USB une fois l'installation terminée.

REMARQUE : Pour configurer la NIC USB en protocole DHCP sous un système d'exploitation Linux ou XenServer, voir la documentation du système d'exploitation ou de l'hyperviseur.

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 dans le dossier `/tmp/` du système d'exploitation hôte ESXi.

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 l'OS et l'iDRAC à l'aide de RACADM

Pour activer ou désactiver la fonction Connexion directe entre le système d'exploitation et l'iDRAC à l'aide de RACADM, utilisez les objets du groupe `iDRAC.OS-BMC`.

Pour plus d'informations, consultez le document Registre d'attributs d'Integrated Dell Remote Access Controller disponible sur la page Manuels iDRAC.

Activation ou désactivation de la connexion directe entre le SE et iDRAC à l'aide de l'utilitaire de paramètres 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 d'iDRAC, accédez à **Autorisations de communication**.
La page **Paramètres iDRAC.Autorisations de communication** 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.

   REMARQUE : Si vous définissez le mode intermédiaire LOM, assurez-vous que :
   - Le système d'exploitation et le contrôleur iDRAC se trouvent sur le même sous-réseau.
   - La sélection de NIC est définie dans les paramètres réseau sur un LOM.

   Pour désactiver cette fonction sélectionnez **Désactivée**.

   REMARQUE : L'option LOM peut être sélectionnée uniquement si la carte prend en charge la capacité de transfert du SE à l'iDRAC. Sinon, cette option est grisée.
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.

   REMARQUE : Si le serveur est connecté en mode LOM partagé, le champ **Adresse IP du SE** est désactivé.
4. Si vous sélectionnez la carte **NIC USB** en tant que configuration de transfert, saisissez l'adresse IP de la carte NIC USB.
   La valeur par défaut est 169.254.1.1. Toutefois, si cette adresse IP est en conflit avec l'adresse IP des autres interfaces du système hôte ou du réseau local, vous devez la modifier. Ne saisissez pas les adresses IP 169.254.0.3 et 169.254.0.4. Ces adresses IP sont réservées au port NIC USB du panneau avant lorsqu'un câble USB Type-C est utilisé.

   REMARQUE : Si IPv6 est préférable, l'adresse par défaut est fde1:53ba:e9a0:de11::1. Si nécessaire, cette adresse peut être modifiée dans le paramètre iDRAC OS-BMC.UsbNicULA. Si IPv6 n'est pas souhaité sur le USB-NIC, il peut être désactivé en modifiant l'adresse en « :: »
5. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

Les informations sont enregistrées.

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

Pour activer la connexion directe entre le système d'exploitation et l'iDRAC à l'aide de l'interface Web, procédez comme suit :

1. Accédez à **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Connexion directe entre le SE et iDRAC**.
   La page **Connexion directe entre le SE et iDRAC** s'affiche.
2. Modifiez l'état à **Activé**.
3. Sélectionnez l'une des options suivantes pour le mode intermédiaire :
   - **LOM** : le lien de connexion directe du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le périphérique LOM ou OCP.
   - **USB** : le lien de connexion directe du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le bus USB interne.

   REMARQUE : Si vous définissez le mode intermédiaire LOM, assurez-vous que :
   - le système d'exploitation et l'iDRAC se trouvent sur le même sous-réseau ;
   - la sélection de la carte réseau dans les paramètres réseau est définie sur LOM.
4. Si le serveur est connecté en mode LOM partagé, le champ **Adresse IP du SE** est désactivé.

   REMARQUE : Si le VLAN est activé sur l'iDRAC, le transfert LOM ne fonctionne qu'en mode LOM partagé avec le marquage VLAN configuré sur l'hôte.

   REMARQUE :
   - Lorsque le mode de connexion directe est configuré sur LOM, le lancement de l'iDRAC à partir du système d'exploitation hôte après un démarrage à froid est impossible.
   - La connexion directe LOM est supprimée à l'aide de la fonction de mode dédié.
5. Si vous sélectionnez la carte **NIC USB** en tant que configuration de transfert, saisissez l'adresse IP de la carte NIC USB.
   La valeur par défaut est 169.254.1.1. Il est recommandé d'utiliser l'adresse IP par défaut. Toutefois, si cette adresse IP est en conflit avec l'adresse IP des autres interfaces du système hôte ou du réseau local, vous devez la modifier.

   Ne saisissez pas les adresses IP 169.254.0.3 et 169.254.0.4. Ces adresses IP sont réservées au port NIC USB du panneau avant lorsqu'un câble USB Type-C est utilisé.

   REMARQUE : Si IPv6 est préférable, l'adresse par défaut est fde1:53ba:e9a0:de11::1. Si nécessaire, cette adresse peut être modifiée dans l'iDRAC. Paramètre OS-BMC.UsbNicULA. Si IPv6 n'est pas souhaité sur le USB-NIC, il peut être désactivé en modifiant l'adresse en « :: »

   REMARQUE : Lorsque vous modifiez l'adresse IP statique de la carte réseau USB, la plage d'adresses DHCP est automatiquement ajustée pour tenir compte de la nouvelle adresse IP statique. Par exemple, si vous définissez l'adresse IP statique sur 169.254.1.1, l'adresse DHCP est mise à jour sur 169.254.1.2. Cette modification est compatible avec le gestionnaire de réseau Wicked, qui accepte la nouvelle adresse DHCP.
6. Cliquez sur **Appliquer**.
7. 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.

Obtention de certificats

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

Tableau 15. 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.

Tableau 15. Types de certificats en fonction du type de connexion (suite)

Type de connexion	Type de certificat	Mode d'obtention
		REMARQUE : 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. **REMARQUE :** 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. **REMARQUE :** 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 :** L'iDRAC est livré avec un certificat de serveur SSL auto-signé par défaut. Le serveur Web, le média virtuel et la console virtuelle de l'iDRAC utilisent ce certificat. **REMARQUE :** Les certificats SHA-2 sont également pris en charge.

Certificats de serveur SSL

iDRAC inclut un serveur web configuré pour utiliser le protocole de sécurité standard SSL lors du transfert de données chiffrées sur un réseau. Une option de cryptage SSL est fournie pour désactiver les chiffrements simples. Le protocole SSL repose sur une technologie de chiffrement asymétrique et fournit une communication chiffrée et authentifiée entre clients et serveurs pour prévenir les écoutes illicites sur les réseaux.

Un système SSL peut effectuer les tâches suivantes :

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

REMARQUE : Si le chiffrement SSL est réglé sur 256 bits ou plus et 168 bits ou plus, les paramètres de cryptographie de l'environnement de votre machine virtuelle (JVM, IcedTea) peuvent exiger l'installation des fichiers Unlimited Strength Java Cryptography Extension Policy pour permettre l'utilisation des plug-ins iDRAC tels que vConsole avec ce niveau de cryptage. Pour en savoir plus sur l'installation des fichiers de règles, voir la documentation Java.

Par défaut, le serveur web iDRAC comprend un certificat numérique SSL auto-signé Dell unique. Vous pouvez remplacer le certificat SSL par défaut par un certificat signé par une autorité de certification (AC) reconnue. Une autorité de certification est une entité commerciale qui répond de manière fiable aux normes exigeantes du secteur des technologies de l'information en matière de filtrage, d'identification et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'autorités de certification. Pour lancer le processus d'obtention d'un certificat signé par une autorité de certification, utilisez l'interface web iDRAC ou RACADM afin de générer une Requête de signature de certificat (CSR) accompagnée des informations relatives à votre société. Soumettez ensuite la requête CSR générée à une autorité de certification telle que VeriSign ou Thawte. L'autorité de certification peut être une autorité de certification racine ou autorité de certification intermédiaire. Après réception du certificat SSL signé par une autorité de certification, chargez-le iDRAC.

Vous pouvez télécharger un certificat d'autorité de certification à partir de l'interface utilisateur de l'iDRAC via **Paramètres iDRAC** > **Services** > **Serveur Web** > **Demande de signature de certificat SSL/TLS**. Vous pouvez également voir les détails du certificat dans d'autres interfaces.

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 avertissements de certificat.

Vous pouvez également télécharger 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 téléchargé 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 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, la confiance doit de nouveau être approuvée entre l'iDRAC et 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'iDRAC 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 tous les iDRAC sont considérés 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 considéré comme fiable par le navigateur. Les iDRAC sont considérés comme fiables par les clients des visionneuses.

Vous pouvez activer la fonctionnalité de notification d'expiration du certificat afin de pouvoir configurer l'intervalle et la fréquence de notification. L'iDRAC fournit une notification sur l'expiration du certificat.

REMARQUE : Les certificats auto-signés par défaut sont automatiquement mis à jour au redémarrage de l'iDRAC, ce qui explique qu'ils ne soient pas pris en compte pour l'expiration du certificat.

Vous pouvez activer la notification d'expiration du certificat et l'intervalle de notification à partir de **Paramètres de l'iDRAC** > **Services** > **Serveur Web** > **Paramètres**. En outre, au bas de la page de connexion de l'iDRAC figure un avertissement de sécurité concernant l'expiration du certificat.

Génération d'une nouvelle demande de signature de certificat

Une CSR est une demande numérique destinée à une autorité de certification (CA) pour obtenir un certificat de serveur SSL. Les certificats de serveur SSL permettent aux clients de serveur de faire confiance à l'identité du serveur et de négocier une session chiffrée avec le serveur.

Lorsque l'autorité de certification reçoit une CSR, 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 CSR et émet le certificat de serveur SSL, celui-ci peut être chargé sur l'iDRAC. Les informations utilisées pour générer la CSR, stockées dans le firmware de l'iDRAC, doivent correspondre aux informations contenues dans le certificat de serveur SSL, à savoir que le certificat doit avoir été généré en utilisant la CSR créée par l'iDRAC.

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

Pour générer un fichier CSR à l'aide de RACADM, utilisez la commande `set` avec les objets du groupe `iDRAC.Security`, puis utilisez la commande `sslcsrgen` pour générer le fichier CSR.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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

Pour générer un fichier RSC :

REMARQUE : Chaque nouvelle CSR remplace toutes les données de CSR précédentes stockées dans le firmware. Les informations contenues dans la CSR doivent correspondre aux informations contenues dans le certificat de serveur SSL. Sinon, iDRAC n'accepte pas le certificat.

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Services** > **Serveur Web** > **Certificat 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.

Pour en savoir plus, voir l'**Aide en ligne d'iDRAC**.

3. Cliquez sur **Générer**.
   Une nouvelle CSR est générée. Enregistrez-la sur la station de gestion.

Inscription automatique de certificats

Dans l'iDRAC, la fonctionnalité d'inscription automatique de certificats (ACE) vous permet d'installer et de renouveler automatiquement les certificats utilisés par le serveur Web. Lorsque cette fonctionnalité est activée, le certificat du serveur Web existant est remplacé par un nouveau certificat. Saisissez les détails de la demande de signature de certificat (CSR) avant d'activer ACE.

REMARQUE :

- ACE est une fonctionnalité sous licence et nécessite une licence Datacenter.
- Une configuration NDES (Service d'enregistrement d'appareils réseau) valide est requise pour la délivrance du certificat du serveur.

L'heure de l'iDRAC doit être synchronisée avec le NDES/l'autorité de certification.

REMARQUE : Si l'heure n'est pas synchronisée, l'iDRAC peut recevoir des certificats non valides ou expirés pendant le processus d'inscription et de renouvellement.

Les paramètres de configuration d'ACE sont les suivants :

- Activer et Désactiver.
- URL de serveur SCEP/ACEM (environnement de gestion automatique des certificats)
- Mot de passe de vérification

REMARQUE : pour plus d'informations sur ces paramètres, voir l'**Aide en ligne de l'iDRAC**.

Vous trouverez ci-dessous les états disponibles pour l'ACE :

- Inscrite : l'ACE est activée. Le certificat est surveillé et le nouveau certificat peut être émis à l'expiration.
- Inscription : l'état intermédiaire après l'activation de l'ACE.
- Erreur : un problème s'est produit avec le serveur NDES.
- Aucun : par défaut.

REMARQUE : Lorsque vous activez l'ACE, le serveur Web est redémarré et toutes les sessions Web existantes sont déconnectées.

REMARQUE : Pour afficher les messages de réussite ou d'échec, consultez les journaux Lifecycle.

Téléversement d'un certificat de serveur

Après avoir généré une demande de signature de certificat (CSR), vous pouvez télécharger le certificat de serveur SSL signé sur le firmware iDRAC. L'iDRAC doit être réinitialisé pour appliquer le certificat. iDRAC n'accepte que les certificats X509, Web server Base 64 encodés. Les certificats SHA-2 sont également pris en charge.

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

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

Pour charger le certificat de serveur SSL, utilisez la commande `sslcertupload`. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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. Téléchargez la clé privée à l'aide de la commande distante `sslkeyupload`.
3. Téléchargez le certificat signé sur l'iDRAC à l'aide de la commande distante `sslcertupload`.
   Le nouveau certificat est chargé dans l'iDRAC. Un message s'affiche vous demandant de réinitialiser l'iDRAC.
4. Exécutez la commande `racreset` RACADM pour réinitialiser l'iDRAC.
   L'iDRAC se réinitialise et le nouveau certificat est appliqué. L'iDRAC devient indisponible pendant quelques minutes lors de la réinitialisation.

REMARQUE : Vous devez réinitialiser l'iDRAC pour appliquer le nouveau certificat. L'ancien certificat reste actif jusqu'à ce que l'iDRAC soit réinitialisé.

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

Pour téléverser un certificat de serveur SSL :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Services** > **Serveur Web** > **Demande de signature de certificat SSL/TLS**, sélectionnez **Télécharger 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 **Appliquer**.
   Le certificat de serveur SSL est téléversé vers iDRAC.
4. Un message contextuel s'affiche pour vous demander de réinitialiser l'iDRAC immédiatement ou ultérieurement. Cliquez sur **Reset iDRAC** or **Reset iDRAC Later** si nécessaire.
   L'iDRAC se réinitialise et le nouveau certificat est appliqué. L'iDRAC devient indisponible pendant quelques minutes lors de la réinitialisation.
   REMARQUE : Vous devez réinitialiser l'iDRAC pour appliquer le nouveau certificat. L'ancien certificat reste actif jusqu'à ce que l'iDRAC soit réinitialisé.

Affichage du certificat de serveur

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

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, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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

Dans l'interface Web d'iDRAC, accédez à **Paramètres iDRAC** > **Services** > **Serveur Web** > **Certificat SSL**. La page **SSL** affiche le certificat de serveur SSL qui est en cours d'utilisation en haut de la page.

Téléversement d'un certificat de signature personnalisée

Vous pouvez charger un certificat de signature personnalisé 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'iDRAC :

1. Accédez à **iDRAC Settings** > **Services** > **Web Server** > **SSL/TLS Custom Signing Certificate**.
   La page **SSL** s'affiche.
2. Sous **SSL/TLS Custom Signing Certificate**, cliquez sur **Charger un certificat de signature**.
   La page **Téléverser le certificat de signature de certificat SSL personnalisé** s'affiche.
3. Cliquez sur **Choose File** et sélectionnez le fichier de 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 vers iDRAC.

6. Un message contextuel s'affiche pour vous demander de réinitialiser l'iDRAC immédiatement ou ultérieurement. Cliquez sur **Reset iDRAC** or **Reset iDRAC Later** si nécessaire.
   Après la réinitialisation de l'iDRAC, le nouveau certificat est appliqué. L'iDRAC devient indisponible pendant quelques minutes lors de la réinitialisation.
   REMARQUE : Vous devez réinitialiser l'iDRAC pour appliquer le nouveau certificat. L'ancien certificat reste actif jusqu'à ce que l'iDRAC soit réinitialisé.

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

Pour charger le certificat de signature de certificat SSL personnalisé à l'aide de RACADM, utilisez la commande `sslcertupload`, puis la commande `racreset` pour réinitialiser l'iDRAC.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Télécharger un certificat de signature de certificat SSL personnalisé

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

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, utilisez la sous-commande `sslcertdownload`. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Téléchargement du certificat de signature personnalisé

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

1. Accédez à **Paramètres iDRAC** > **Connectivité** > **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.

Télécharger un certificat de signature de certificat SSL personnalisé

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

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, utilisez la sous-commande `sslcertdownload`. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Téléchargement du certificat de signature personnalisé

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

1. Accédez à **Paramètres iDRAC** > **Connectivité** > **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.

Configuration de plusieurs iDRAC à l'aide de RACADM

À l'aide de RACADM, vous pouvez configurer un ou plusieurs contrôleurs iDRAC avec des propriétés identiques. Lorsque vous interrogez un iDRAC spécifique en utilisant son ID de groupe et son ID d'objet, RACADM crée un fichier de configuration à partir des informations récupérées. Importez le fichier vers les autres iDRAC pour les configurer de façon identique.

REMARQUE :

- Le fichier de configuration contient des informations applicables au serveur spécifique. Les informations sont organisées sous différents groupes d'objets.
- Quelques fichiers de configuration contiennent des informations iDRAC uniques (telles que l'adresse IP statique) que vous devez modifier avant d'importer le fichier dans les autres iDRAC.

Vous pouvez également utiliser le profil de configuration du système (SCP) pour configurer plusieurs iDRAC à l'aide de RACADM. Le fichier SCP contient les informations relatives à la configuration des composants. Vous pouvez utiliser ce fichier pour appliquer la configuration des BIOS, iDRAC, RAID et NIC en important le fichier dans un système cible. Pour plus d'informations, voir le livre blanc **Flux de travail de la configuration XML** disponible sur Page de manuels Dell.

Pour configurer plusieurs iDRAC à l'aide du fichier de configuration :

1. Interrogez l'iDRAC cible qui contient la configuration nécessaire en utilisant la commande suivante :

   ```
   racadm get -f <file_name>.xml -t xml -c iDRAC.Embedded.1
   ```

   La commande demande la configuration iDRAC et génère le fichier de configuration.

   REMARQUE : La redirection de la configuration iDRAC vers un fichier à l'aide de `get -f` n'est prise en charge qu'avec les interfaces RACADM locales et distantes.

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

   La commande `get` 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.

2. Si nécessaire, modifiez le fichier de configuration à l'aide d'un éditeur de texte.

   REMARQUE : Il est recommandé de modifier ce fichier avec un simple éditeur de texte. L'utilitaire RACADM utilise un analyseur de texte ASCII. Tout formatage risque de perturber l'analyseur et de corrompre la base de données RACADM.

3. Sur l'iDRAC cible, utilisez la commande suivante pour modifier les paramètres :

   ```
   racadm set -f <file_name>.xml -t xml
   ```

   Cela provoque le chargement des informations dans l'autre iDRAC. Vous pouvez utiliser la commande `set` pour synchroniser la base de données des utilisateurs et des mots de passe avec Server Administrator.

4. Réinitialisez l'iDRAC cible à l'aide de la commande : `racadm racreset`

Désactivation de l'accès pour modifier les paramètres de configuration iDRAC sur un système hôte

Vous pouvez désactiver l'accès pour modifier les paramètres de configuration de l'iDRAC via l'interface RACADM locale ou l'utilitaire de configuration de l'iDRAC. Vous pouvez néanmoins afficher ces paramètres de configuration. Pour ce faire, procédez comme suit :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Services** > **Configurations locales**.
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 ou IPMITool pour configurer l'iDRAC. Vous pouvez toutefois utiliser IPMI sur LAN.

8

Autorisation déléguée à l'aide d'OAuth 2.0

La fonctionnalité d'autorisation déléguée permet à un utilisateur ou une console d'accéder à l'API iDRAC à l'aide de JSON Web de jetons (JWT) OAuth 2.0 que l'utilisateur ou la console obtient d'abord auprès d'un serveur d'autorisation. Lorsqu'un JWT OAuth est récupéré, l'utilisateur ou la console peut l'utiliser pour appeler l'API iDRAC. Cela évite d'avoir à spécifier le nom d'utilisateur et le mot de passe pour accéder à l'API.

REMARQUE : Cette fonctionnalité est disponible uniquement pour la licence DataCenter. Vous devez disposer du privilège de configuration iDRAC ou de configuration des utilisateurs pour pouvoir utiliser cette fonctionnalité.

iDRAC prend en charge la configuration d'un maximum de 2 serveurs d'autorisation. La configuration exige qu'un utilisateur spécifie les informations suivantes sur le serveur d'autorisation :

- **Nom** : chaîne permettant d'identifier le serveur d'autorisation sur l'iDRAC.
- **URL de métadonnées** : l'URL conforme à OpenID Connect, telle qu'annoncée par le serveur.
- **Certificat HTTPS** : clé publique de serveur que l'iDRAC doit utiliser pour communiquer avec le serveur.
- **Clé hors ligne** : document défini par le JWK pour le serveur d'autorisation.
- **Émetteur hors ligne** : chaîne de l'émetteur telle qu'utilisée dans les jetons émis par le serveur d'autorisation.

Pour la configuration en ligne :

- Lors de la configuration d'un serveur d'autorisation, l'administrateur de l'iDRAC doit s'assurer que l'iDRAC dispose d'un accès réseau en ligne au serveur d'autorisation.
- Si l'iDRAC ne parvient pas à accéder au serveur d'autorisation, la configuration échoue et une tentative ultérieure d'accès à l'API iDRAC échoue même si un jeton valide est présenté.

Pour la configuration hors ligne :

- L'iDRAC n'a pas besoin de communiquer avec le serveur d'authentification, mais il est configuré avec les informations de métadonnées qu'il a téléchargées hors ligne. Lorsqu'il est configuré hors ligne, l'iDRAC possède la partie publique des clés de signature et peut valider le jeton sans connexion réseau au serveur d'authentification.

9

Affichage des informations d'iDRAC et d'un système géré

Vous pouvez afficher l'intégrité et les propriétés de l'iDRAC et d'un système géré, l'inventaire du matériel et des firmwares, l'intégrité des capteurs, les périphériques de stockage, les périphériques réseau et afficher les sessions utilisateur et y mettre fin.

Sujets :

Affichage de l'intégrité et des propriétés d'un système géré

Lorsque vous ouvrez une session dans l'interface Web d'iDRAC, la page **Récapitulatif du système** permet de visualiser l'intégrité du système géré et les informations iDRAC 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 voyants LED du panneau avant et la réinitialisation d'iDRAC.

Pour accéder à la page **Récapitulatif du système**, accédez à **Système** > **Aperçu** > **Récapitulatif**. La page du **Résumé du système** s'affiche. Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.

Vous pouvez également afficher les informations de base du récapitulatif du système en utilisant l'utilitaire de configuration de l'iDRAC. Pour ce faire, dans l'utilitaire de configuration de l'iDRAC, accédez à **Récapitulatif du système**. La page **Récapitulatif du système des paramètres de l'iDRAC** s'affiche. Pour plus d'informations, voir **l'aide en ligne de l'utilitaire de configuration l'iDRAC**.

Configuration du suivi des actifs

La fonctionnalité Suivi des actifs dans l'iDRAC vous offre la possibilité de configurer divers attributs qui sont associés à votre serveur. Cela comprend des informations telles que l'acquisition, la garantie, le service, etc.

REMARQUE : La fonctionnalité Suivi des actifs dans l'iDRAC est similaire à la fonctionnalité Numéro d'inventaire dans OpenManage Server Administrator. Cependant, les informations sur les attributs doivent être saisies séparément dans les deux outils afin de rapporter les données d'actif pertinentes.

Pour configurer le suivi des actifs :

1. Dans l'interface de l'iDRAC, accédez à **Configuration** > **Suivi des actifs**.

2. Cliquez sur **Ajouter des actifs personnalisés** pour ajouter des attributs supplémentaires qui ne sont pas spécifiés par défaut sur cette page.
3. Saisissez toutes les informations pertinentes sur les actifs de votre serveur et cliquez sur **Appliquer**.
4. Pour afficher le rapport de suivi des actifs, accédez à **Système** > **Détails** > **Suivi des actifs**.

Affichage de l'inventaire du système

Vous pouvez afficher des informations sur les composants matériels et les firmwares installés sur le système géré. Pour afficher l'inventaire système dans l'interface Web de l'iDRAC, accédez à **Système** > **Inventaire**. Pour plus d'informations sur les propriétés affichées, voir l'**Aide en ligne de l'iDRAC**.

La section **Inventaire de matériel** affiche les informations sur les composants suivants disponibles sur le système géré :

- iDRAC
- OEM
- Contrôleur RAID
- Batteries
- CPU
- Processeur graphique
- DIMM
- Disque durs
- Fonds de panier
- Cartes d'interface réseau (incorporées et intégrées)
- Carte vidéo
- Unité d'alimentation (PSU)
- Ventilateurs
- Adaptateurs HBA Fibre Channel
- USB
- Périphériques SSD PCIe NVMe

REMARQUE : Dans l'inventaire matériel d'un processeur graphique, les entrées BuildDate, GPUGUID et OEMInfo sont prises en charge et renseignées pour les appareils NVIDIA uniquement. Les données OEMInfo sont renseignées uniquement s'il existe des données fournies par l'appareil NVIDIA pour ce champ.

Le tableau suivant dresse la liste des attributs et les valeurs attendues dans la page **Inventaire du matériel** dans l'interface utilisateur de l'iDRAC lorsque la carte DPU Pensando ne prend pas en charge HII.

Tableau 16. Attributs et valeurs attendues

Attributs	Valeur attendue
CurrentMACAddress	Vide
BusNumber	Zéro
DataBusWidth	Vide
PCIDeviceID	Vide
PCISubDeviceID	Vide
PCISubVendorID	Vide
PCIVendorID	Vide
SlotLength	Vide
SlotType	Vide
LastSystemInventoryTime	1970-01-01T00:00:00
LastUpdateTime	1970-01-01T00:00:00
FCoEOffloadMode	Désactivé
iScsiOffloadMode	Désactivé

Tableau 16. Attributs et valeurs attendues (suite)

Attributs	Valeur attendue
NicMode	Désactivé
MaxBandwidth	0
MinBandwidth	0

REMARQUE : L'inventaire différé est mis à jour uniquement après le démarrage de l'hôte. Les inventaires tels que les logements PCIe et les appareils PCIe dans l'inventaire du matériel font partie de l'inventaire différé qui est généré lors du démarrage de l'hôte (après l'opération CSIOR). Le retrait ou l'enfichage à chaud des disques ne modifie pas les données d'inventaire, sauf si l'hôte est redémarré.

Sur la page **Périphérique réseau** > **État de la partition** de l'interface utilisateur, les valeurs ID d'appareil PCI, Bande passante minimale et Bande passante maximale sont vides.

Sur la page **Périphérique réseau** > **Paramètres et fonctionnalités**, la valeur Protocole de démarrage pris en charge est vide.

La section **Inventaire de firmware** affiche la version de firmware des composants suivants :

- BIOS
- Lifecycle Controller
- iDRAC
- Pack de pilotes de système d'exploitation
- FPGA
- Contrôleurs PERC
- Disques physiques
- Alimentation
- Carte NIC
- Fibre Channel
- Fond de panier
- Boîtier
- Cartes SSD PCIe
- TPM
- iSM

REMARQUE : Les composants qui ne disposent pas de la fonctionnalité de restauration via l'iDRAC n'affichent pas leur date de publication dans l'inventaire des logiciels. Lorsqu'un composant est mis à jour à partir du système d'exploitation hôte, il est impossible de spécifier le contenu de la restauration et les détails de la date de publication.

REMARQUE : Après avoir effectué une mise à jour intrabande du firmware du système d'exploitation sur un boîtier externe (JBOD), effectuez un redémarrage à froid (un cycle d'alimentation) du serveur pour mettre à jour les informations du boîtier et l'inventaire du système dans l'iDRAC.

REMARQUE : L'inventaire des firmwares peut prendre beaucoup de temps ou ne pas s'afficher dans certains cas. Utilisez la commande RACADM `getremoteservicestatus` avant d'exécuter l'inventaire des firmwares.

REMARQUE :

- L'inventaire des logiciels affiche uniquement les 4 derniers octets de la version du firmware, ainsi que la date de publication. Par exemple, si la version du micrologiciel est FLVDL06, l'inventaire du micrologiciel affiche DL06.
- Pour les disques SATA, la version du firmware affiche toujours quatre caractères. Si un disque SATA présente une version du firmware à plus de quatre caractères, l'inventaire des logiciels affiche les quatre derniers caractères de la version du firmware et de la page de stockage, tandis que l'inventaire du matériel affiche la version complète.
- Lors de l'affichage de l'inventaire des logiciels à l'aide de l'interface Redfish, la date de publication s'affiche uniquement pour les composants prenant en charge la restauration.

REMARQUE :

- La version du firmware de l'offre groupée de processeur graphique s'affiche au format 00.00.00.00 :
  - jusqu'à la mise à jour du firmware à l'aide du package DUP ;
  - après l'exécution de System Erase sur le système.

- En cas d'échec de communication entre la carte de base du processeur graphique et l'iDRAC, la version de l'offre groupée de processeur graphique peut ne pas s'afficher dans l'inventaire des firmwares. Pour résoudre le problème de communication, effectuez un cycle d'alimentation. La version du firmware s'affiche au format 00.00.00.00 lorsque la communication est restaurée.
- Si un appareil (par exemple : TPM) est hors tension, l'inventaire des logiciels indique que la version est **Indisponible** ou affiche **0**. Et si l'application n'est pas installée, la version indique **Non installé.**
- Le système affiche la date et l'heure initiales par défaut du système dans le champ **Date/Heure d'installation** de la page **Inventaire système**, jusqu'à ce qu'une nouvelle version du firmware de l'appareil soit installée à l'aide du package DUP. En outre, la date et l'heure du BIOS et de l'iDRAC doivent être synchronisées pour les composants dont les détails d'inventaire sont obtenus à partir du BIOS (par exemple : BIOS, TPM).
- La date d'installation ne change pas si la version mise à jour est identique à la version installée.
- Il est parfois possible que le champ **LastUpdateTime** d'un composant de l'inventaire du matériel de l'iDRAC s'affiche sous forme de date ultérieure/antérieure, notamment lorsque la date du BIOS ou de l'hôte est définie sur une date incorrecte. Pour résoudre ce problème, corrigez la date du BIOS ou de l'hôte.

Lorsque vous remplacez un composant matériel ou mettez à jour les versions du firmware, activez et exécutez l'option **Collecter l'inventaire système au redémarrage** (CSIOR). Après quelques minutes, ouvrez une session iDRAC et accédez à la page **Inventaire système** pour afficher les détails. La disponibilité des informations peut prendre jusqu'à cinq minutes en fonction du matériel installé sur le serveur.

REMARQUE : L'option CSIOR est activée par défaut.

REMARQUE : Les modifications de la configuration et les mises à jour du micrologiciel effectuées au sein du système d'exploitation peuvent ne pas être reflétées correctement dans l'inventaire tant que vous ne redémarrez pas le serveur.

Cliquez sur **Exporter** pour exporter l'inventaire de matériel au format XML et l'enregistrer à un emplacement de votre choix.

Affichage des composants du système

Les composants suivants de l'interface utilisateur de l'iDRAC vous aident à surveiller l'intégrité d'un système géré :

- **Batteries** : fournit des informations sur les batteries CMOS de la carte système et le RAID de stockage sur la carte mère.

  REMARQUE : Les paramètres de la batterie ROMB de stockage sont disponibles uniquement si le système dispose d'une carte ROMB avec une batterie.

- **Processeur** : indique l'intégrité et l'état des processeurs dans un système géré. Il signale également la régulation automatique du processeur et les échecs prédictifs.
- **Mémoire** : affiche l'intégrité et l'état des modules DIMM (Dual In-line Memory Module) présents sur le système géré.
- **Intrusion** : fournit des informations sur le châssis.
- **Alimentation** (disponible uniquement sur les serveurs au format rack et les serveurs tours) : fournit des informations sur les blocs d'alimentation et l'état de redondance de ces blocs.

  REMARQUE : Si le système est doté d'un seul bloc d'alimentation, la redondance de bloc est **désactivée**.

- **Tension** : indique l'état et les valeurs des capteurs de tension des divers composants du système.
- **Refroidissement** : fournit des détails sur les températures des ventilateurs et des composants matériels. Les quatre types de ventilateurs sont les suivants : double rotor groupé (ventilateur 1A, ventilateur 1B), rotor simple groupé (ventilateur 1A, ventilateur 1B), double rotor non groupé (ventilateur 1, ventilateur 2) et rotor simple non groupé (ventilateur 1, ventilateur 2).
- **Accélérateur** : fournit des détails sur les processeurs graphiques et les accélérateurs de traitement.
- **Logements PCIe** : fournit des détails sur tous les périphériques PCIe, y compris les cartes SSD PCIe (NVMe).
- **Périphériques réseau** : fournit des détails sur tous les périphériques réseau, y compris les DPU.

Le tableau suivant répertorie les composants système qu'il est possible de surveiller :

REMARQUE : La page **Présentation du système** contient uniquement les données relatives aux capteurs présents sur votre système.

Tableau 17. Composants système surveillés à partir de l'interface utilisateur de l'iDRAC

Composants du système	Chemin de navigation dans l'iDRAC
Batteries	**Système** > **Présentation** > **Batteries**
Refroidissement	**Système** > **Présentation** > **Refroidissement**
Processeur	**Système** > **Présentation** > **Processeur**
Mémoire	**Système** > **Présentation** > **Mémoire**
Intrusion	**Système** > **Présentation** > **Intrusion**
Alimentation	**Système** > **Présentation** > **Alimentation**
Supports amovibles	**Système** > **Présentation** > **Support amovible**
Tensions	**Système** > **Présentation** > **Tensions**
Périphériques réseau	**Système** > **Présentation** > **Périphériques réseau**
Accélérateurs	**Système** > **Présentation** > **Accélérateurs**
Logements PCIe	**Système** > **Présentation** > **Logements PCIe**

Utilisez la commande `racadm getsensorinfo` pour obtenir les détails de chacun de ces composants.

REMARQUE : Pour plus d'informations sur les propriétés prises en charge et leurs valeurs, consultez l'**aide en ligne de l'iDRAC**.

Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'entrée/sortie

Dans les serveurs PowerEdge, Intel ME prend en charge l'utilisation du calcul par seconde (Compute Usage Per Second, CUPS). La fonctionnalité CUPS assure une surveillance en temps réel de l'indice d'utilisation du processeur, de la mémoire, des E/S et du système. Intel ME prend en charge une surveillance des performances hors bande (OOB) et ne consomme pas de ressources processeur. Intel ME dispose d'un capteur CUPS système qui fournit des valeurs de calcul, de mémoire et d'utilisation des ressources d'E/S sous forme d'index CUPS. L'iDRAC surveille cet indice CUPS pour l'utilisation globale du système et surveille également l'indice d'utilisation instantanée du processeur, de la mémoire et des E/S.

Le processeur et le chipset possèdent des compteurs de surveillance des ressources (RMC) dédiés. Les données provenant de ces RMC sont interrogées afin d'obtenir des informations sur l'utilisation des ressources système. Les données envoyées par les RMC sont agrégées par le gestionnaire de nœuds afin de mesurer l'utilisation cumulée de chacune de ces ressources système, telle qu'elle est lue par iDRAC à l'aide de mécanismes d'intercommunication existants pour fournir des données via des interfaces de gestion hors bande.

Les paramètres de performances et les valeurs d'indice représentés par le capteur Intel s'appliquent à l'ensemble du système physique. Par conséquent, la représentation des données de performance sur les interfaces concerne l'ensemble du système physique, même si le système est virtualisé et s'il dispose de plusieurs hôtes virtuels.

Pour afficher les paramètres de performances, les capteurs pris en charge des capteurs doivent être présents sur le serveur.

Les quatre paramètres d'utilisation du système sont les suivants :

- **Utilisation du processeur** : les données fournies par les RMC pour chaque cœur de processeur sont agrégées afin de produire une valeur d'utilisation cumulée pour tous les cœurs du système. Cette utilisation est basée sur le temps passé à l'état actif et à l'état inactif. Un échantillon de RMC est réalisé toutes les six secondes.
- **Utilisation de la mémoire** : les RMC mesurent le trafic de la mémoire sur chaque canal de mémoire ou instance de contrôleur de mémoire. Les données de ces RMC sont agrégées pour mesurer le trafic cumulé de la mémoire sur tous les canaux de mémoire du système. Il s'agit d'une mesure de la consommation de la bande passante de la mémoire et non du taux d'utilisation de la mémoire. L'iDRAC l'agrège pendant une minute, de sorte à correspondre ou non à l'utilisation de la mémoire affichée par d'autres outils du système d'exploitation, tels que **top** dans Linux. L'utilisation de la bande passante de mémoire indiquée par iDRAC permet de savoir si la charge applicative consomme ou non beaucoup de mémoire.
- **Utilisation des E/S** : il y a un RMC par port racine dans le contrôleur PERC (PCI Express Root Complex) pour mesurer le trafic PCI Express en provenance ou à destination de ce port racine et du segment inférieur. Les données de ces RMC sont agrégées afin de mesurer le trafic PCI Express de tous les segments PCI Express émanant du package. Il s'agit de mesurer l'utilisation de la bande passante d'E/S du système.

- **Indice CUPS au niveau du système** : l'indice CUPS est calculé en agrégeant les indices du processeur, de la mémoire et des E/S, en prenant en compte le facteur de charge de chaque ressource système. Le facteur de charge varie en fonction de la nature de la charge applicative sur le système. L'indice CUPS représente une mesure de la marge de calcul disponible sur le serveur. Si le système présente un indice CUPS élevé, cela signifie qu'il y a peu de marge pour augmenter la charge applicative sur ce système. Plus la consommation des ressources diminue, plus l'indice CUPS système est faible. Un faible indice CUPS indique qu'il existe une grande marge de calcul, que le serveur peut recevoir de nouvelles charges applicatives et que le serveur est en mode basse consommation pour réduire sa consommation électrique. La surveillance des charges applicatives peut ensuite être appliquée à travers le datacenter afin de fournir une vue globale de la charge applicative du datacenter, de manière à obtenir une solution de datacenter dynamique.

REMARQUE : Les indices d'utilisation du processeur, de la mémoire et des E/S sont agrégés sur un intervalle d'une minute. Autrement dit, si ces indices rencontrent des pics instantanés, ceux-ci peuvent être supprimés. Les indices permettent de représenter des schémas de charge applicative, et non le taux d'utilisation des ressources.

Les traps IPMI, SEL et SNMP sont générés si les seuils des indices d'utilisation sont atteints et que les événements de capteur sont activés. Les balises d'événement de capteur sont désactivées par défaut. Elles peuvent être activées à l'aide de l'interface IPMI standard.

Les privilèges requis sont les suivants :

- Le droit de connexion est requis pour surveiller les données de performances.
- Le droit de configuration est requis pour définir des seuils d'avertissement et réinitialiser l'historique des pics.
- Le privilège d'ouverture de session et une licence Enterprise sont requis pour pouvoir lire les données de l'historique des statistiques.

Surveillance de l'indice de performance de l'UC, de la mémoire et des modules d'E/S à l'aide de RACADM

Utilisez la sous-commande **SystemPerfStatistics** pour surveiller l'indice de performance de l'UC, de la mémoire et des modules d'E/S. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'entrée/sortie à l'aide de l'interface Web

Pour surveiller l'indice de performances du processeur, de la mémoire et des modules d'E/S, accédez à **Système** > **Performances** dans l'interface Web de l'iDRAC.

- Section **Performances système** : affiche la mesure actuelle et la mesure d'avertissement de l'UC, de l'indice d'utilisation de mémoire et d'E/S et de l'indice CUPS au niveau du système dans une vue graphique.
- Section **Historique de données des performances système** :
  - fournit les statistiques concernant l'utilisation du processeur, de la mémoire et des E/S et l'indice CUPS au niveau du système. Si le système hôte est mis hors tension, le graphique affiche la puissance hors ligne inférieure à 0 %.
  - Vous pouvez réinitialiser les valeurs maximales d'utilisation d'un capteur particulier. Cliquez sur **Réinitialiser les valeurs historiques maximales**. Vous devez disposer de privilèges de configuration pour réinitialiser la valeur maximale.
- Section **Mesures de performances** :
  - Afficher l'état et la valeur actuelle.
  - Affiche ou spécifie la limite d'utilisation de seuil d'avertissement. Vous devez disposer du privilège de configuration du serveur pour définir les valeurs de seuil.

Pour plus d'informations sur les propriétés affichées, voir l'**aide en ligne d'iDRAC**.

Lecture des inventaires des firmwares et du matériel

REMARQUE : Laissez quelques secondes de délai lors de l'utilisation de la commande `getremoteservicesstatus`. Le délai d'expiration est de 5 minutes.

1. Utilisez la méthode/URI/commande `getremoteservicesstatus` pour vérifier si le Lifecycle Controller (LC) est prêt. Assurez-vous que le système a été mis **sous tension** au moins une fois et que l'option **Collecter l'inventaire système au redémarrage (CSIOR)** a été exécutée au moins une fois pour obtenir les informations appropriées. En fonction de la configuration requise pour certains composants tels que le stockage et le réseau, vous devrez peut-être également vérifier si le système est sur l'état **Hors POST** et **Temps réel (RT).**
2. Le délai d'expiration maximal pour que LC soit prêt devrait être de 5 minutes. Assurez-vous que le système est sur l'état suivant pour que le LC soit prêt :

- Hors POST
- La tâche n'est pas déjà en cours d'exécution
- Pas dans l'interface utilisateur LC
- Hôte bloqué sur POST

3. Une fois que le LC est prêt, utilisez la méthode/URI/commande `getinventory`.

Exécution et vérification de l'état de la configuration du système/composant

REMARQUE : Laissez quelques secondes de délai lors de l'utilisation de la commande `getremoteservicesstatus`. Le délai d'expiration est de 5 minutes.

1. Vérifiez l'inventaire du firmware (suivez la procédure mentionnée ci-dessus).
2. Pour éviter d'éventuelles défaillances ultérieures, assurez-vous que le composant obligatoire est présent dans le système.
3. Après les vérifications initiales, utilisez la méthode/URI/commande `getremoteservicesstatus` pour vérifier si le LC est prêt. En fonction de la configuration requise pour certains composants tels que le stockage et le réseau, vous devrez peut-être également vérifier si le système est défini sur l'état **Hors POST** et **Temps réel (RT)**.
4. Une fois le LC prêt, utilisez les configurations du système/composant et créez la tâche.
5. Créez une tâche de redémarrage ou redémarrez l'hôte si la configuration nécessite un redémarrage de l'hôte. Un paramètre de configuration spécifique peut nécessiter un redémarrage à froid.
6. L'appelant doit vérifier l'état de la tâche à exécuter : **Réussite/Échec**. Affichez les événements du journal Lifecycle, l'état de la file d'attente des tâches et vérifiez les résultats de la configuration pour plus de détails sur les échecs.
7. Ce n'est qu'après avoir **collecté l'inventaire système au redémarrage (CSIOR)** sur l'hôte, le cas échéant, que la tâche est marquée comme terminée si elle n'a pas échoué. Cela s'applique si un redémarrage de l'hôte est nécessaire.
8. Une fois la tâche terminée, attendez 30 secondes, puis utilisez la méthode/URI/commande `getremoteservicesstatus` pour vérifier si le LC est prêt, avec d'autres états requis, puis lisez les valeurs attendues.

Exécution et vérification de l'état de la mise à jour de firmware

REMARQUE : Laissez quelques secondes de délai lors de l'utilisation de la commande `getremoteservicesstatus`. Le délai d'expiration est de 5 minutes.

1. Vérifiez l'inventaire du firmware (suivez la procédure mentionnée ci-dessus).
2. Pour éviter d'éventuelles défaillances ultérieures, vérifiez si le composant à mettre à jour est présent dans le système et/ou si le Dell Update Package (DUP) pris en charge a bien été sélectionné pour téléchargement.
3. Après les vérifications initiales, utilisez la méthode/URI/commande `getremoteservicesstatus` pour vérifier si le LC est prêt.
4. Une fois le LC prêt, utilisez la méthode/URI/commande `firmwareupdate` et exécutez le DUP approprié pour démarrer la mise à jour.
5. Si la mise à jour nécessite un redémarrage de l'hôte, créez une tâche de redémarrage ou redémarrez l'hôte. Les mises à jour de gestion de l'alimentation, OSM et PERC nécessitent un redémarrage à froid.
6. Vérifiez l'état de la tâche **: Réussite/Échec**. Affichez les événements du journal Lifecycle et l'état de la file d'attente des tâches, et recherchez les résultats de configuration pour obtenir plus de détails sur les échecs.
7. Ce n'est qu'après avoir **collecté l'inventaire système au redémarrage (CSIOR)** sur l'hôte, le cas échéant, que la tâche est marquée comme terminée si elle n'a pas échoué, même lorsqu'il y a plusieurs mises à jour de catalogues. Par conséquent, il est recommandé que l'appelant n'ait pas de délai d'expiration propre ou que celui-ci soit supérieur à ce délai.
8. Si la mise à jour est bloquée pendant plus de 6 heures (par exemple, le module de tâche n'obtient pas l'état du module de mise à jour pendant 6 heures), la tâche peut expirer et échouer.
9. Les délais d'expiration des mises à jour sont basés sur les recommandations de l'équipe chargée des périphériques, qui sont lues au moment de l'exécution.
10. Une fois la tâche marquée comme terminée et si l'inventaire ne signale pas que de nouvelles modifications viennent d'être appliquées, attendez 30 s, puis vérifiez à nouveau l'inventaire.

Détection de serveur inactif

L'iDRAC fournit un index de surveillance des performances hors bande des composants du serveur, comme le processeur, la mémoire et les E/S.

Les données d'historique de l'index CUPS au niveau du serveur sont utilisées pour déterminer si le serveur est utilisé ou inactif depuis une longue période. Si le serveur est sous-utilisé, c'est-à-dire sous un certain seuil depuis une période définie (en heures), il sera signalé comme serveur inactif.

Cette fonction est prise en charge uniquement sur les plates-formes Intel disposant de la fonctionnalité CUPS. Les plates-formes AMD et Intel sans fonctionnalité CUPS ne prennent pas en charge cette fonction.

REMARQUE :

- Cette fonctionnalité nécessite une licence Datacenter.
- Pour lire les configurations des paramètres Configuration du serveur inactif, vous devez disposer des privilèges de connexion et pour modifier les paramètres, vous devez disposer du privilège de configuration de l'iDRAC.

Pour afficher ou modifier les paramètres, accédez à **Configuration** > **Paramètres système**.

La détection de serveur inactif est signalée en fonction des paramètres suivants :

- Seuil de serveur inactif (%) : défini sur 20 % par défaut. Il peut être configuré entre 0 et 50 %. L'opération de réinitialisation définit le seuil sur 20 %.
- Intervalle d'analyse de serveur actif (en heures) : il s'agit de la période sur laquelle les échantillons horaires sont collectés pour déterminer l'inactivité du serveur. Cette option est définie sur 240 heures par défaut et peut être configurée de 1 à 9 000 heures. L'opération de réinitialisation définit l'intervalle sur 240 heures.
- Utilisation du serveur en percentile (%) : la valeur d'utilisation en percentile peut être définie entre 80 et 100 %. La valeur par défaut est 80 %. Si 80 % des échantillons horaires tombent en dessous du seuil d'utilisation, le serveur est considéré comme inactif.

Modification des paramètres de détection de serveur inactif à l'aide de RACADM

```
racadm get system.idleServerDetection
```

Modification des paramètres de détection de serveur inactif à l'aide de Redfish

```
https://<iDRAC IP>/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/
System.Embedded.1
```

Gestion des processeurs graphiques (accélérateurs)

Les serveurs Dell PowerEdge sont expédiés avec un processeur graphique. La gestion des processeurs graphiques vous permet d'afficher les différents processeurs graphiques connectés au système et de surveiller les informations relatives à l'alimentation, à la température et aux données thermiques des processeurs graphiques.

Vous trouverez ci-dessous les propriétés du processeur graphique et les détails des licences :

Tableau 18. Propriétés du processeur graphique et détails des licences

Propriétés des modules GPU	Licence
Inventaire	
Numéro de référence de la carte	Toutes les licences
Informations OEM	Toutes les licences
Numéro de série	Toutes les licences

Tableau 18. Propriétés du processeur graphique et détails des licences (suite)

Propriétés des modules GPU	Licence
Nom marketing	Toutes les licences
Numéro de référence du processeur graphique	Toutes les licences
Date de la version	Toutes les licences
Version du firmware	Toutes les licences
GUID du processeur graphique	Toutes les licences
ID fournisseur PCI	Toutes les licences
ID appareil PCI	Toutes les licences
ID sous-fournisseur PCI	Toutes les licences
ID sous-appareil PCI	Toutes les licences
État du module GPU	Toutes les licences
Intégrité du lecteur de processeur graphique	Toutes les licences
Mesures thermiques	
Température du processeur graphique principal	Toutes les licences
Température du processeur graphique secondaire	Toutes les licences
Température de la carte système	Toutes les licences
Température de la mémoire	Toutes les licences
Température minimale de ralentissement du processeur graphique	Enterprise
Arrêt de la température du processeur graphique	Enterprise
Température maximale de fonctionnement de la mémoire	Enterprise
Température maximale de fonctionnement du processeur graphique	Enterprise
État d'alerte thermique	Enterprise
État du frein de l'alimentation	Enterprise
Mesures d'alimentation	
Consommation électrique	Toutes les licences
Condition des blocs d'alimentation	Enterprise
États des blocs d'alimentation de la carte système	Enterprise

REMARQUE :

- Les propriétés des processeurs graphiques ne sont pas répertoriées pour les cartes de processeur graphique intégrées et l'état est signalé comme **inconnu**.
- La température de fonctionnement peut être différente pour les systèmes basés sur AMD.
- Le nombre d'entrées de processeur graphique par logement PCIe affiché sur l'hôte peut être différent de celui de l'iDRAC.
- Lorsqu'un cycle marche/arrêt manuel est nécessaire après l'exécution de mises à jour de composants ou de firmware groupés pour les FPGA des processeurs graphiques ou de la carte de distribution de l'alimentation (PDB), l'événement SUP0545 s'affiche dans les journaux Lifecycle (LC). Après cet événement, assurez-vous d'effectuer un cycle marche/arrêt manuel ou virtuel pour éviter tout comportement inattendu sur le serveur.
- Après une mise à jour de firmware du processeur graphique qui inclut des mises à jour de firmware des composants ou des mises à jour de firmware groupées, assurez-vous d'exécuter un cycle d'alimentation secteur manuel ou virtuel pour terminer la mise à jour. Cela permet d'éviter tout comportement inattendu lié aux processeurs graphiques dans l'iDRAC.

- En mode persistant, lors du redémarrage à chaud, les valeurs limites de recours aux seuils énergétiques du processeur graphique peuvent ne pas être exactes.
- La fonctionnalité de recours aux seuils énergétiques du processeur graphique n'est pas disponible dans les configurations de processeur graphique autres qu'A2.

Le processeur graphique doit être à l'état Prêt avant que la commande ne récupère les données. Le champ GPUStatus de l'inventaire indique la disponibilité du processeur graphique et si l'appareil du processeur graphique répond ou non. Si l'état du processeur graphique est Prêt, GPUStatus affiche **OK**. Sinon, l'état indique **Non disponible**.

Le processeur graphique propose plusieurs paramètres d'intégrité qui peuvent être extraits via l'interface SMBPB des contrôleurs NVIDIA. Cette fonctionnalité est limitée uniquement aux cartes NVIDIA. Vous trouverez ci-dessous les paramètres d'intégrité récupérés à partir du processeur graphique :

- Alimentation
- Température
- Caractéristiques thermiques

REMARQUE : Cette fonctionnalité est limitée uniquement aux cartes NVIDIA. Ces informations ne sont pas disponibles pour les autres processeurs graphiques pouvant être pris en charge par le serveur. L'intervalle d'interrogation des cartes des processeurs graphiques sur le PBI est de 5 secondes.

Avec un redémarrage à chaud et le mode persistant désactivé, nous pouvons observer le comportement suivant :

- La consommation électrique est S/O.
- La limite de seuil énergétique s'affiche avec les anciennes valeurs limites de l'inventaire.

Le pilote de processeur graphique NVIDIA doit être installé et en cours d'exécution sur le système hôte pour que diverses fonctionnalités du processeur graphique soient disponibles. Exemples de fonctionnalités de processeur graphique disponibles : consommation électrique, limite de capacité énergétique actuelle, plafonnement et limitation de l'alimentation du processeur graphique, température cible du processeur graphique, température de ralentissement minimale du processeur graphique, température d'arrêt du processeur graphique, température de fonctionnement maximale de la mémoire, température de fonctionnement maximale du processeur graphique, utilisation du processeur graphique, etc. Ces valeurs s'affichent comme **S/O** si le pilote du processeur graphique NVIDIA n'est pas installé. Les fonctionnalités du processeur graphique qui dépendent du pilote chargé et en cours d'exécution ne figurent pas toutes sur cette liste.

Dans Linux, lorsque la carte n'est pas utilisée, le pilote sous-alimente la carte et se décharge pour économiser de l'énergie. Dans ces cas, les fonctionnalités de consommation électrique, limite de capacité énergétique actuelle, plafonnement et limitation de l'alimentation du processeur graphique, température cible du processeur graphique, température de ralentissement minimale du processeur graphique, température d'arrêt du processeur graphique, température de fonctionnement maximale de la mémoire, température de fonctionnement maximale du processeur graphique, utilisation du processeur graphique et d'autres fonctionnalités ne sont pas disponibles. Le mode persistant doit être activé pour que le périphérique ne puisse pas se décharger. Vous pouvez utiliser l'outil nvidia-smi pour activer cette option à l'aide de la commande `nvidia-smi -pm 1`.

Vous pouvez générer des rapports du processeur graphique à l'aide de la télémétrie. Pour plus d'informations sur les fonctionnalités de télémétrie, voir Streaming de télémétrie.

REMARQUE : Dans Racadm, vous pouvez voir des entrées de processeur graphique factices avec des valeurs vides. Cela peut se produire si l'appareil n'est pas prêt à répondre quand l'iDRAC interroge le processeur graphique pour obtenir des informations. Exécutez une opération `racrest` d'iDRAC pour résoudre ce problème.

Surveillance des accélérateurs de traitement

Les appareils dotés d'accélérateurs de traitement de classe PCIe ont besoin d'une surveillance en temps réel de la température et des capteurs, car ils génèrent une chaleur importante au cours de leur utilisation.

Procédez comme suit pour obtenir des informations sur l'inventaire des **accélérateurs de traitement** :

1. Mettez le serveur hors tension.
2. Installez les accélérateurs sur la carte de montage.
3. Mettez le serveur sous tension.
4. Patientez jusqu'à la fin de l'autotest de démarrage.
5. Connectez-vous à l'interface utilisateur de l'iDRAC.
6. Accédez à **Système** > **Présentation** > **Accélérateurs**. Vous pouvez voir les sections Processeur graphique et Accélérateurs de traitement.
7. Développez l'accélérateur spécifique pour afficher les informations de capteur suivantes :
   - Consommation électrique
   - Détails de la température

REMARQUE : Les capteurs de température logiques ne sont pas affichés dans les interfaces de l'iDRAC. Seuls les capteurs de température physiques sont affichés.

REMARQUE : Vous devez disposer de droits de connexion iDRAC pour accéder aux informations des accélérateurs.

REMARQUE : Les capteurs de consommation électrique sont disponibles uniquement pour les accélérateurs pris en charge et uniquement avec la licence Datacenter.

REMARQUE : Les interfaces de l'iDRAC peuvent ne pas afficher les informations des capteurs d'alimentation et thermiques qui dépendent du système d'exploitation hôte (système d'exploitation). Dans ce cas, installez les pilotes du processeur graphique (package ROCm) dans le système d'exploitation hôte.

REMARQUE :

- Il est recommandé d'exécuter la mise à jour du firmware CEC du processeur graphique A100 avant celle du firmware des accélérateurs.
- N'exécutez pas simultanément la mise à jour du firmware CEC du processeur graphique et des accélérateurs, afin d'éviter l'échec des mises à jour. Exécutez un cycle d'alimentation secteur manuel ou virtuel après les échecs de mise à jour de firmware. Cela permet d'éviter d'autres échecs de mise à jour unique causés par l'échec de la mise à jour précédente.
- La mise à jour du firmware FPGA de la carte mère HGX A100 8-GPU peut prendre entre 60 et 90 minutes.
- Les mises à jour du DUP FPGA et CEC de la carte mère HGX A100 8-GPU ne doivent pas être déclenchées simultanément. Il est recommandé de suivre ces étapes :
  1. Mettez à jour le firmware CEC.
  2. Effectuez un cycle d'alimentation virtuel ou un cycle d'alimentation manuel.
  3. Mettez à jour le firmware FPGA.
  4. Effectuez un autre cycle d'alimentation virtuel ou un autre cycle d'alimentation manuel.
- Pour mettre à jour le PDB FPGA à partir du système d'exploitation, effectuez un redémarrage à froid. Après la mise à jour, un cycle d'alimentation virtuel est exécuté.

REMARQUE : Parfois, les accélérateurs envoient des valeurs de consommation électrique égales à 0. Par conséquent, PLDM utilise également des valeurs égales à 0 et affiche ces mêmes valeurs dans l'interface utilisateur. Les valeurs sont automatiquement corrigées dans les relevés suivants.

REMARQUE : Les périphériques PCIe dépendent des pilotes et du firmware des appareils pour répondre aux demandes de l'iDRAC. Ces appareils consignent le message LC HWC9053 (perte de communication avec l'appareil) lorsque les pilotes et le firmware requis ne sont pas chargés ou lorsque le serveur se trouve dans l'environnement pré-système d'exploitation (shell UEFI et page Lifecycle Controller).

Vérification de la conformité du système aux normes Fresh Air

Le refroidissement Fresh Air utilise directement l'air extérieur pour refroidir les systèmes du datacenter. Les systèmes conformes à la norme Fresh Air peuvent fonctionner au-dessus de la plage ambiante normale (températures allant jusqu'à 45 °C (113 °F)).

REMARQUE : Certains serveurs ou certaines configurations de serveur peuvent ne pas être conformes à la norme Fresh Air. Voir le manuel du serveur pour plus d'informations sur la conformité Fresh Air ou contactez Dell.

Pour vérifier la conformité du système aux normes Fresh Air :

1. Dans l'interface Web de l'iDRAC, accédez à **Système** > **Présentation** > **Refroidissement** > **Présentation de la température**. La page **Présentation de la température** 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 suivre le temps de fonctionnement du système (en pourcentage) à une température ambiante supérieure au seuil de température Fresh Air normalement toléré. La valeur du capteur de température de la carte système est collectée sur une certaine période

de temps pour surveiller la température. La collecte de données commence lorsque le système est mis sous tension après sa livraison de l'usine. Les données sont collectées et affichées tant que le système reste sous tension. Vous pouvez suivre et enregistrer la température surveillée au cours des sept dernières années.

REMARQUE : Vous pouvez suivre l'historique des températures, même pour les systèmes qui ne sont pas conformes aux normes Fresh Air. Toutefois, les limites de seuil et les avertissements générés liés à la qualité de l'air ambiant sont basés sur les limites prises en charge par les normes Fresh Air. Les limites sont de 42 °C pour les bandes d'avertissement et de 47 °C pour les bandes critiques. Ces valeurs correspondent aux limites Fresh Air de 40 °C et 45 °C avec une marge de 2 °C.

Deux bandes de température fixes associées aux limites d'air frais sont suivies :

- Bande d'avertissement : indique la durée pendant laquelle un système a fonctionné au-dessus du seuil d'avertissement du capteur de température (42 °C). Le système peut fonctionner dans la bande d'avertissement durant 10 % du temps pendant 12 mois.
- Bande critique : désigne la durée pendant laquelle un système a fonctionné au-dessus du seuil critique du capteur de température (47 °C). Le système peut fonctionner dans la bande critique durant 1 % du temps pendant 12 mois, ce qui augmente également le temps dans la bande d'avertissement.

Les données collectées sont représentées sous forme graphique pour suivre les niveaux de 10 % et de 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 à une température supérieure au seuil normalement toléré pour une période de fonctionnement précise. Si la température moyenne de la période de fonctionnement précise est supérieure ou égale au niveau d'avertissement (> = 8 %) ou au niveau critique (> = 0,8 %), un événement est consigné 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 au moins 8 % du temps au cours des 12 derniers mois.
- Événement critique lorsque la température d'entrée a été supérieure au seuil d'avertissement durant au moins 10 % du temps au cours des 12 derniers mois.
- Événement d'avertissement lorsque la température d'entrée a été supérieure au seuil critique durant au moins 0,8 % du temps au cours des 12 derniers mois.
- Événement critique lorsque la température d'entrée a été supérieure au seuil critique durant au moins 1 % du temps au cours des 12 derniers mois.

Vous pouvez également configurer l'iDRAC pour générer des événements supplémentaires. Pour plus d'informations, reportez-vous à la section Définition d'événement de récurrence d'alerte.

Affichage des données historiques de température à l'aide de l'interface RACADM

Pour afficher des données historiques à l'aide de l'interface RACADM, utilisez la commande `inlettemphistory`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

REMARQUE : Vous pouvez constater des incohérences entre les valeurs de température d'entrée dans l'interface utilisateur de l'iDRAC et dans l'interface RACADM. Pour comparer les données entre ces interfaces, veuillez noter les points suivants :

- Options de l'**interface utilisateur de l'iDRAC** dans la liste déroulante et sorties correspondantes :
  - Dernier jour : données horaires affichées pour les dernières 24 heures.
  - Mois dernier : données quotidiennes affichées pour les 30 derniers jours.
  - Année dernière : données mensuelles affichées pour les 12 derniers mois.
- Sortie de l'interface **RACADM** : affiche les valeurs exactes pour les heures, jours, mois et années des commandes RACADM respectives.

Affichage des données historiques de température à l'aide de l'interface Web iDRAC

Pour afficher les données historiques de température :

1. Dans l'interface Web de l'iDRAC, accédez à **Système** > **Présentation** > **Refroidissement** > **Présentation de la température**. La page **Présentation de la température** s'affiche.

2. Reportez-vous à la section **Données historiques de températures de la carte système** qui fournit un affichage graphique des températures 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 de l'iDRAC**.

   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.

   REMARQUE : Actuellement, la carte GPU AMD WX3200 ne prend pas en charge l'interface I2C pour les capteurs de température. Par conséquent, les relevés de température ne sont pas disponibles pour cette carte à partir des interfaces de l'iDRAC.

Configuration du seuil d'avertissement de température d'entrée

Vous pouvez modifier les valeurs de seuil d'avertissement minimale et maximale pour le capteur de température d'entrée de la carte système. Si l'action de réinitialisation des valeurs par défaut est effectuée, les seuils de température sont définis sur ces valeurs par défaut. Vous devez disposer du privilège de configuration pour définir les valeurs de seuil d'avertissement du capteur de température d'entrée.

REMARQUE : La différence entre **Avertissement supérieur** et **Lecture** de **Température d'entrée de la carte système** doit être supérieure à 2 degrés pour éviter tout avertissement d'état d'intégrité.

REMARQUE : À chaque fois que vous redémarrez le système ou mettez à jour le firmware de l'iDRAC, les journaux LC qui fournissent des informations sur la limite de seuil définie pour le capteur de température d'entrée s'affichent.

Configuration du seuil d'avertissement de température d'entrée à l'aide de l'interface Web

Pour configurer le seuil d'avertissement de la température d'entrée :

1. Dans l'interface Web de l'iDRAC, accédez à **Système** > **Présentation** > **Refroidissement** > **Présentation de la température**. La page **Présentation de la température** s'affiche.
2. Dans la section **Capteurs de température**, saisissez les valeurs minimale et maximale du **Seuil d'avertissement** en degrés Celsius ou Fahrenheit pour la **Température d'entrée de la carte système**. Si vous saisissez la valeur en degrés Celsius, le système calcule et affiche automatiquement la valeur en degrés Fahrenheit. De la même façon, si vous saisissez la valeur en degrés Fahrenheit, la valeur en degrés Celsius s'affiche.
3. Cliquez sur **Appliquer**.

   Les valeurs sont configurées.

   REMARQUE : Les modifications apportées aux seuils par défaut ne sont pas reflétées dans le graphique de données historiques car les limites du graphique s'appliquent uniquement aux valeurs limites d'air frais. Les avertissements pour dépassement des seuils personnalisés sont différents de ceux associés au dépassement des seuils d'air frais.

Affichage des interfaces réseau disponibles sur le SE hôte

Vous pouvez consulter les informations sur toutes les interfaces réseau disponibles sur le système d'exploitation hôte, telles que les adresses IP attribuées au serveur. L'iDRAC Service Module fournit ces informations à l'iDRAC. Les informations relatives à l'adresse IP du système d'exploitation incluent les adresses IPv4 et IPv6, l'adresse MAC, le masque de sous-réseau ou la longueur de préfixe, le FQDD du périphérique réseau, le nom de l'interface réseau, la description de l'interface réseau, l'état de l'interface réseau, le type de l'interface réseau (Ethernet, tunnel, bouclage, etc.), les adresses de passerelle, les adresses de serveur DNS et les adresses de serveur DHCP.

REMARQUE : Cette fonctionnalité est disponible sous les licences iDRAC Express et Enterprise/Datacenter.

Pour afficher les informations de système d'exploitation, assurez-vous que :

- Vous disposez des privilèges de connexion.

- L'iDRAC Service Module est installé sur le système d'exploitation hôte et en cours de fonctionnement.
- L'option Informations sur le SE est activée dans la page **Paramètres iDRAC** > **Présentation** > **iDRAC Service Module**.

iDRAC peut afficher les adresses IPv4 et IPv6 de toutes les interfaces configurées sur le SE hôte.

En fonction de la manière dont le système d'exploitation d'hôte détecte le serveur DHCP, l'adresse du serveur DHCP IPv4 ou IPv6 peut ne pas s'afficher.

Affichage des interfaces réseau disponibles sur l'OS hôte à l'aide de RACADM

Utilisez la commande `gethostnetworkinterfaces` pour afficher les interfaces réseau disponibles sur les systèmes d'exploitation hôtes à l'aide de RACADM. Pour en savoir plus, voir le *Guide de l'interface de ligne de commande RACADM d'iDRAC*.

Affichage des interfaces réseau disponibles sur l'OS hôte à l'aide de l'interface web

Pour afficher les interfaces réseau disponibles sur l'OS hôte à l'aide de l'interface web :

1. Accédez à **Système** > **OS hôte** > **Interfaces réseau**.
   La page **Interfaces réseau** affiche toutes les interfaces réseau disponibles sur le système d'exploitation hôte.
2. Pour afficher la liste des interfaces réseau associées à un périphérique réseau, à partir du menu déroulant **FQDD de périphérique réseau**, sélectionnez un périphérique réseau, puis cliquez sur **Appliquer**.
   Les détails de l'adresse IP de l'OS sont affichés dans la section **Interfaces réseau de l'OS hôte**.
3. Dans la colonne **FQDD de périphérique**, cliquez sur le lien du périphérique réseau.
   La page de l'appareil correspondant s'affiche à partir de la section **Matériel** > **Périphériques réseau**, où vous pouvez afficher les détails de l'appareil. Pour plus d'informations sur les propriétés, voir l'**Aide en ligne de l'iDRAC**.
4. Cliquez sur l'icône + pour afficher plus de détails.
   De même, sur la page **Matériel** > **Périphériques réseau**, vous pouvez afficher les informations d'interface réseau de l'OS hôte associées à un périphérique réseau. Cliquez sur **Afficher les interfaces réseau du système d'exploitation hôte**.
   REMARQUE : Pour le système d'exploitation de l'hôte ESXi dans iDRAC Service Module v2.3.0 ou ultérieure, la colonne **Description** dans la liste **Détails supplémentaires** s'affiche au format suivant :

   ```
   <List-of-Uplinks-Configured-on-the-vSwitch>/<Port-Group>/<Interface-name>
   ```

Affichage ou fin des sessions iDRAC

Vous pouvez afficher le nombre d'utilisateurs actuellement connectés à iDRAC et mettre fin aux sessions utilisateur.

Fin des sessions iDRAC à l'aide de RACADM

Vous devez disposer des privilèges d'administrateur pour pouvoir mettre fin aux sessions iDRAC à l'aide de 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, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Fin des sessions iDRAC à l'aide de l'interface Web

Les utilisateurs ne disposant pas de privilèges d'administrateur doivent disposer du privilège de configuration iDRAC pour pouvoir mettre fin aux sessions iDRAC à l'aide de l'interface Web d'iDRAC.

Pour afficher les sessions iDRAC et y mettre fin :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **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 de l'iDRAC**.
2. Pour mettre fin à la session, dans la colonne **Annuler**, cliquez sur l'icône de corbeille pour la session.

10

Configuration de la communication iDRAC

Vous pouvez communiquer avec iDRAC en utilisant les modes suivants :

- Interface web iDRAC
- Connexion série à l'aide d'un câble DB9 (RAC série ou IPMI série). 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
- Remote Services

REMARQUE : Pour vous assurer que les commandes d'importation et d'exportation de l'interface RACADM locale fonctionnent correctement, vérifiez que l'hôte de stockage de masse USB est activé sur le système d'exploitation. Pour plus d'informations sur l'activation de l'hôte de stockage USB, consultez la documentation de votre système d'exploitation.

Le tableau suivant offre un aperçu des protocoles pris en charge, des commandes prises en charge et des conditions requises :

Tableau 19. Modes de communication — Résumé

Mode de communication	Protocole pris en charge	Commandes prises en charge	Prérequis
Interface web iDRAC	Internet Protocol (https)	S/O	Serveur Web
Série en utilisant un câble Null modem DB9	Protocole série	RACADM et IPMI	Activation d'une partie du firmware de l'iDRAC et de RAC série ou de IPMI série
IPMI série sur LAN	Protocole IPMB (Intelligent Platform Management Bus) SSH	IPMI	IPMITool est installé et IPMI série sur LAN est activé
IPMI sur le LAN	Protocole IPMB (Intelligent Platform Management Bus)	IPMI	IPMITool est installé et les paramètres IPMI sont activés
Interface RACADM distante	HTTPS	Interface RACADM distante	L'interface distance RACADM est installée et activée
firmware RACADM	SSH	firmware RACADM	Le firmware RACADM est installé et activé.
Interface RACADM locale	IPMI	Interface RACADM locale	L'interface RACADM locale est installée
Services distants [1]	Redfish	Divers plug-in de navigateur, CURL (Windows et Linux), demande Python et modules JSON	Des Plug-in, CURL, les modules Python sont installés
[1] Pour plus d'informations, consultez le document *Guide de l'utilisateur de Dell Lifecycle Controller* disponible à l'adresse des manuels iDRAC.			

Sujets :

- Communication avec l'iDRAC via une connexion série à l'aide d'un câble DB9
- Permutation entre RAC Série et la console série à l'aide d'un câble DB9
- Communication avec l'iDRAC à l'aide de SOL IPMI
- Communication avec l'iDRAC à l'aide d'IPMI sur LAN
- Activation ou désactivation de l'interface distante RACADM
- Désactivation de l'interface locale RACADM
- Configuration de Linux pour la console série pendant le démarrage sous RHEL

- Configuration du terminal série sous RHEL
- Schémas cryptographiques SSH pris en charge

Communication avec l'iDRAC via une connexion série à l'aide d'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
- Série IPMI : mode de base de connexion directe et mode terminal de connexion directe.

REMARQUE : Lorsque USB DB9 est connecté au système, le **Débit en bauds** (**Paramètres iDRAC** > **Connectivité** > **Série**) est réglé automatiquement en fonction de l'activation ou non de **RAC série**. Si **RAC série** est activé, le paramètre **RAC série > Débit en bauds** est défini pour USB DB9. Si **RAC série** est désactivé (IPMI activé), **IPMI série > Débit en bauds** est défini pour USB DB9.

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.

   REMARQUE : Un cycle de marche/arrêt du serveur est nécessaire à partir de vConsole ou de l'interface utilisateur pour toute modification du débit en bauds.

   REMARQUE : Si l'authentification de connexion en série de l'iDRAC est désactivée, la réinitialisation de l'iDRAC est nécessaire pour toute modification du débit en bauds.

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 la phase du processus de démarrage du système géré, vous pouvez voir l'écran du POST ou celui du système d'exploitation. Cela dépend de la configuration : console SAC pour Windows et écrans en mode texte Linux pour Linux.

4. Activez les connexions RAC série ou IPMI série dans iDRAC.

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 du BIOS du système** > **Communication série**.
4. Sélectionnez **Connecteur série externe** vers **périphérique d'accès distant**.
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 iDRAC.

REMARQUE : Ces informations s'appliquent uniquement à iDRAC sur des serveurs en rack et de type tour.

Activation de la connexion RAC série à l'aide de RACADM

Pour activer la connexion série RAC à l'aide de RACADM, utilisez la commande `set` avec l'objet du groupe `iDRAC.Serial`.

Activation de la connexion RAC série à l'aide de l'interface Web

Pour activer la connexion RAC série :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Réseau** > **Série**.
   La page **Série** s'affiche.
2. Sous **RAC série**, sélectionnez **Activé** et spécifiez les valeurs des attributs.
3. Cliquez sur **Appliquer**.
   Les paramètres série RAC sont configurés.

Activation des modes de base et terminal de connexion série IPMI

Pour activer le routage série IPMI du BIOS vers iDRAC, configurez IPMI série dans les modes suivants dans iDRAC :

REMARQUE : Ces informations s'appliquent uniquement à iDRAC sur des serveurs en rack et de type tour.

- Mode de base IPMI : prend en charge une interface binaire pour l'accès aux programmes, comme le shell IPMI (ipmish) qui est inclus dans l'utilitaire de gestion de la carte mère (BMU). Par exemple, pour imprimer le journal des événements système à l'aide du script ipmish via le mode de base IPMI, exécutez la commande suivante : `ipmish -com 1 -baud 57600 -flow cts -u <username> -p <password> sel get`

  REMARQUE : Par défaut, le nom d'utilisateur et le mot de passe iDRAC sont fournis sur le badge du système.

- Mode Terminal IPMI : prend en charge les commandes ASCII envoyées à partir d'un terminal série. Ce mode prend en charge un nombre limité de commandes (notamment le contrôle de l'alimentation) et les commandes IPMI brutes saisies sous forme de caractères ASCII hexadécimaux. Cela vous permet d'afficher les séquences de démarrage du système d'exploitation jusqu'au BIOS, lorsque vous vous connectez à l'iDRAC via SSH. Vous devez vous déconnecter du terminal IPMI à l'aide de la commande `[sys pwd -x]`. Vous trouverez ci-dessous des exemples de commandes du mode Terminal IPMI.
  - `[sys tmode]`
  - `[sys pwd -u root calvin]`
  - `[sys health query -v]`
  - `[18 00 01]`
  - `[sys pwd -x]`

Activation d'une connexion série à l'aide de 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 de l'iDRAC, accédez à **Paramètres iDRAC** > **Connectivité** > **Série**.
2. Sous **IPMI sériel**, spécifiez les valeurs des attributs. Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.
3. Cliquez sur **Appliquer**.

Activation du mode IPMI de connexion série à l'aide de RACADM

Pour configurer le mode IPMI, désactivez l'interface série RAC, puis activez le mode IPMI.

```
racadm set iDRAC.Serial.Enable 0
racadm set iDRAC.IPMISerial.ConnectionMode <n>
```

n=0 – mode Terminal

n=1 – mode de base

Activation des paramètres série IPMI de connexion série à l'aide de l'interface RACADM

1. Remplacez le mode de connexion série IPMI par le paramètre approprié en utilisant la commande.

```
racadm set iDRAC.Serial.Enable 0
```

2. Définissez le débit en bauds des communications IPMI série en utilisant la commande.

```
racadm set iDRAC.IPMISerial.BaudRate <baud_rate>
```

Paramètre	Valeurs autorisées (en bits/s)
<baud_rate>	9600, 19200, 57600 et 115200.

3. Activez le contrôle du débit matériel des communications IPMI série en utilisant la commande.

```
racadm set iDRAC.IPMISerial.FlowContro 1
```

4. Définissez le niveau minimal de privilège pour le canal des communications IPMI série en utilisant la commande.

```
racadm set iDRAC.IPMISerial.ChanPrivLimit <level>
```

Paramètre	Niveau de privilège
<level> = 2	Utilisateur
<level> = 3	Opérateur
<level> = 4	Administrateur

5. Vérifiez que le connecteur MUX (connecteur série externe) est correctement défini vers le périphérique d'accès distant 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 de paramètres supplémentaires pour le mode Terminal IPMI série à láide de RACADM

Pour configurer les paramètres du mode terminal, utilisez la commande `set` avec les objets du groupe `idrac.ipmiserial`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Définition d'autres paramètres pour le mode Terminal IPMI série à l'aide de l'interface Web

Pour définir les paramètres du mode Terminal série :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Connectivité** > **Série**.
   La page **Série** s'affiche.
2. Activez l'option Série IMP.
3. Cliquez sur **Paramètres du mode terminal.**
   La page **Paramètres du mode terminal** s'affiche.
4. Définissez les valeurs 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'iDRAC**.

5. Cliquez sur **Appliquer**.
   Les paramètres du mode Terminal sont définis.
6. Vérifiez que le connecteur MUX (connecteur série externe) est correctement défini sur le périphérique d'accès distant dans le programme de configuration du BIOS pour configurer le BIOS pour la connexion série.

Permutation entre RAC Série et la console série à l'aide d'un câble DB9

iDRAC 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 du mode RAC Série au mode Console série

Pour passer au mode console série lorsque vous vous trouvez en mode communication d'interface série du RAC, appuyez sur la séquence de touches Échap+Maj, Q.

Lorsque vous utilisez le mode terminal, pour passer en mode console série, appuyez sur la séquence de touches Échap+Maj, Q.

Pour revenir au mode terminal, lorsque vous êtes connecté en mode console série, appuyez sur la séquence de touches Échap+Maj, 9.

Passage du mode console série au mode série RAC

Pour passer au mode communication d'interface série du RAC lorsque vous vous trouvez en mode console série, appuyez sur la séquence de touches Échap+Maj, 9.

La séquence de touches vous dirige vers l'invite `iDRAC Login` (si l'iDRAC est défini sur en mode série RAC) ou active le mode Connexion série, où il est possible d'émettre des commandes de terminal si l'iDRAC est défini sur le mode Terminal de connexion directe série IPMI.

Communication avec l'iDRAC à l'aide de SOL IPMI

IPMI série sur LAN permet la redirection des données série de la console texte d'un système géré sur un réseau de gestion Ethernet hors bande partagé ou dédié d'iDRAC. SOL vous permet de :

- 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 iDRAC pour utiliser SOL.
3. Activez un protocole pris en charge (SSH, IPMItool).

Configuration du 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 du 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** est également défini sur 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**.

REMARQUE : Le BIOS envoie les données série de l'écran au format 25 x 80. La fenêtre SSH utilisée pour appeler la commande `console com2` doit être définie sur 25 x 80. L'écran redirigé s'affiche alors correctement.

REMARQUE : Si le chargeur de démarrage ou le système d'exploitation assure la redirection série, comme c'est le cas de GRUB ou Linux, le paramètre BIOS **Redirection After Boot (Redirection après démarrage)** doit être désactivé. Cela évite que plusieurs composants se fassent concurrence pour accéder au port série.

Configuration d'iDRAC pour utiliser SOL

Vous pouvez définir les paramètres SOL dans iDRAC à l'aide de l'interface Web, RACADM ou l'utilitaire de configuration d'iDRAC.

Configuration d'iDRAC pour utiliser SOL à l'aide de RACADM

Pour configurer IPMI sur le LAN (SOL) :

1. Activez IPMI série sur le LAN en utilisant la commande.

```
racadm set iDRAC.IPMISol.Enable 1
```

2. Mettez à jour le niveau minimum de privilège SOL IPMI à l'aide de la commande.

```
racadm set iDRAC.IPMISol.MinPrivilege <level>
```

Paramètre	Niveau de privilège
<level> = 2	Utilisateur
<level> = 3	Opérateur
<level> = 4	Administrateur

REMARQUE : Pour activer SOL IPMI, vous devez disposer du privilège minimal défini dans SOL IPMI. Pour plus d'informations, voir la spécification IPMI 2.0.

3. Modifiez le débit en bauds SOL IPMI à l'aide de la commande.

```
racadm set iDRAC.IPMISol.BaudRate <baud_rate>
```

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

Paramètre	Valeurs autorisées (en bits/s)
<baud_rate>	9600, 19200, 57600 et 115200.

4. Activez SOL pour chaque utilisateur à l'aide de la commande.

```
racadm set iDRAC.Users.<id>.SolEnable 2
```

Paramètre	Description
<id>	ID unique de l'utilisateur

REMARQUE : Pour rediriger la console série sur le réseau local, assurez-vous que le débit (en bauds) des communications SOL est identique au débit (en bauds) du système géré.

Configuration d'iDRAC pour utiliser SOL à l'aide de l'interface Web iDRAC

Pour configurer IPMI sur le LAN (SOL) :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Connectivité** > **Série sur 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 contribuent à améliorer les performances.

   Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

Activation du protocole pris en charge

Les protocoles de chiffrement pris en charge sont IPMI et SSH.

Activation d'un protocole compatible à l'aide de RACADM

Pour activer le SSH, exécutez la commande suivante.

SSH

```
racadm set iDRAC.SSH.Enable 1
```

Pour modifier le port SSH, exécutez la commande suivante :

```
racadm set iDRAC.SSH.Port <port number>
```

Vous pouvez utiliser les outils suivants, entre autres :

- IPMItool pour utilisation du protocole IPMI
- Putty/OpenSSH pour utilisation du protocole SSH

Activation d'un protocole pris en charge à l'aide de l'interface Web

Pour activer SSH, accédez à **Paramètres iDRAC** > **Services** et sélectionnez **Activé** pour SSH.

Pour activer IPMI, accédez à **Paramètres iDRAC** > **Connectivité** et sélectionnez **Paramètres IPMI**. Vérifiez que la valeur **Clé de chiffrement** correspond à des zéros ou appuyez sur la touche Retour arrière pour effacer la valeur et remplacer la valeur par des caractères NULL.

SOL utilisant le protocole IPMI

L'utilitaire SOL basé sur IPMI et IPMItool utilisent RMCP+ avec des datagrammes UDP (port 623). Le protocole RMCP+ offre de meilleures performances en matière d'authentification, de contrôle de l'intégrité des données et de chiffrement, et peut transmettre plusieurs types de charges utiles sur IPMI 2.0. Pour plus d'informations, voir **http://ipmitool.sourceforge.net/manpage.html**.

RMCP+ utilise une clé de chiffrement 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+ au contrôleur iDRAC doit être chiffrée en utilisant la clé de chiffrement (clé du générateur de clé). Vous pouvez définir la clé de chiffrement à l'aide de l'interface Web du contrôleur iDRAC ou l'utilitaire de configuration du contrôleur iDRAC.

Pour démarrer une session SOL en utilisant IPMItool depuis une station de gestion :

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente par défaut des sessions SOL sous **Paramètres iDRAC** > **Services**.

1. Installez IPMITool à partir du DVD **Dell Systems Management Tools and Documentation**.
   Pour les instructions d'installation, voir le **Guide d'installation rapide du logiciel**.
2. À l'invite de commande (Windows ou Linux), exécutez la commande suivante pour démarrer SOL via iDRAC :

   ```
   ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate
   ```

   Cette commande a connecté la station de gestion au port série du système géré.
3. Pour quitter une session SOL dans IPMItool, appuyez sur ~ puis sur . (point).

   REMARQUE : Si une session SOL ne se termine pas, réinitialisez iDRAC et attendez la fin du redémarrage qui peut prendre jusqu'à deux minutes.

REMARQUE : La session SOL IPMI peut s'arrêter pendant la copie d'un long texte de saisie depuis un client exécutant le système d'exploitation Windows vers un système hôte sous Linux. Pour éviter que la session ne se termine brusquement, convertissez n'importe quel texte long en terminaison de ligne de type UNIX.

REMARQUE : Si une session SOL créée à l'aide de l'outil RACADM existe, le fait de démarrer une autre session SOL à l'aide de l'outil IPMI n'affichera aucune notification ou erreur au sujet des sessions existantes.

REMARQUE : En raison des paramètres du système d'exploitation Windows, la session SOL connectée via SSH et l'outil IPMI peuvent afficher un écran vide après le démarrage. Déconnectez et reconnectez la session SOL pour revenir à l'invite de la console SAC.

SOL utilisant SSH

SSH (Secure Shell) est un protocole réseau qui permet d'exécuter des communications avec l'iDRAC via la ligne de commande. Vous pouvez analyser les commandes RACADM via cette interface.

SSH a amélioré la sécurité. L'iDRAC prend uniquement en charge SSH version 2 avec authentification par mot de passe et est activé par défaut. L'iDRAC prend en charge jusqu'à deux à quatre sessions SSH à la fois.

REMARQUE : Lors de l'établissement d'une connexion SSH, un message de sécurité `Further Authentication required` s'affiche même si l'authentification à deux facteurs (2FA) est désactivée.

Utilisez des programmes Open Source, tels que PuTTY ou OpenSSH, qui prennent en charge SSH sur une station de gestion, pour vous connecter à l'iDRAC.

REMARQUE : Exécutez `OpenSSH` à partir d'un émulateur de terminal VT100 ou ANSI sous Windows. L'exécution de `OpenSSH` à l'invite de commande Windows n'offre pas des fonctionnalités complètes (quelques touches ne répondent pas et aucune image n'est affichée).

Avant d'utiliser SSH pour communiquer avec l'iDRAC, procédez comme suit :

1. Configurer le BIOS pour activer la console série
2. Configurer SOL dans iDRAC
3. Activer SSH en utilisant l'interface Web iDRAC ou RACADM

   Client SSH (port 22) > **Connexion WAN** > **iDRAC**

Le SOL basé sur IPMI, qui utilise le protocole SSH, évite d'avoir à utiliser un utilitaire supplémentaire, car la conversion série-réseau s'effectue dans l'iDRAC. La console SSH que vous utilisez doit être capable d'interpréter les données issues du port série du système géré et d'y répondre. Le port série se connecte généralement à un environnement shell qui émule un terminal ANSI ou VT100/VT220. La console série est redirigée automatiquement vers SSH.

Utilisation de SOL depuis OpenSSH sous Linux

Pour démarrer SOL depuis OpenSSH sur une station de gestion Linux :

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente par défaut des sessions SSH sous **Paramètres iDRAC** > **Services**.

1. Démarrez un shell.
2. Connectez-vous à l'iDRAC à l'aide de la commande suivante : ssh **<adresse-ip-iDRAC>** -l **<nom de la connexion>**
3. Entrez l'une des commandes suivantes depuis l'invite de commande pour démarrer SOL :
   - `connect com2`
   - `console com2`

   Cette commande connecte l'iDRAC au port SOL du système géré. Lorsqu'une session SOL est établie, la console de ligne de commande de l'iDRAC n'est pas disponible. Suivez correctement la séquence d'échappement pour ouvrir la console de ligne de commande de l'iDRAC. La séquence d'échappement s'affiche également à l'écran dès qu'une session SOL est connectée. Lorsque le système géré est hors tension, un certain temps est nécessaire pour établir la session SOL.

   REMARQUE : Vous pouvez utiliser la console com1 ou com2 pour démarrer SOL. Redémarrez le serveur pour établir la connexion.

   Pour afficher l'historique de l'interface SOL, activez la capture de données série. Toutes les données série reçues de l'hôte sont alors écrites dans la mémoire de l'iDRAC dans une fenêtre glissante de 512 Ko. Cette fonctionnalité nécessite une licence Datacenter.
4. Quittez la session SOL pour fermer une session SOL active.

Utilisation de SOL depuis PuTTY sous Windows

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente par défaut des sessions SSH sous **Paramètres iDRAC** > **Services**.

Pour démarrer SOL IPMI depuis PuTTY sur une station de gestion Windows :

1. Exécutez la commande suivante pour vous connecter à iDRAC

```
putty.exe [-ssh] <login name>@<iDRAC-ip-address> <port number>
```

   REMARQUE : Le numéro de port est facultatif. Il est requis uniquement lorsque le numéro de port est réaffecté.
2. Exécutez la commande `console com2` ou `connect com2` pour démarrer SOL et le système géré.

   Une session SOL est ouverte de la station de gestion vers le système géré à l'aide du protocole SSH. Pour accéder à la console de ligne de commande de l'iDRAC, suivez la séquence de touches ÉCHAP. Comportement de connexion 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 numérique dans putty sont définies sur :
     - VT100+ — F2 passe, mais pas F12
     - ESC[n~ — F12 passe, mais pas F2
   - Dans Windows, si la console Emergency Management Services (EMS) est ouverte immédiatement après un redémarrage de l'hôte, le terminal Special Admin Console (SAC) peut être corrompu. Quittez la session SOL, fermez le terminal, ouvrez un autre terminal, puis démarrez la session SOL à l'aide de la même commande.

   REMARQUE : En raison des paramètres du système d'exploitation Windows, la session SOL connectée via SSH et l'outil IPMI peuvent afficher un écran vide après le démarrage. Déconnectez et reconnectez la session SOL pour revenir à l'invite de la console SAC.

Déconnexion d'une session SOL dans la console de ligne de commande d'iDRAC

Les commandes de déconnexion d'une session SOL sont basées sur l'utilitaire. Vous pouvez quitter l'utilitaire uniquement lorsqu'une session SOL est complètement terminée.

Pour déconnecter une session SOL, mettez fin à cette session à partir de la console de ligne de commande d'iDRAC :

Pour quitter la redirection SOL, appuyez sur Entrée, puis sur Échap, T.
La session SOL se ferme.

Si une session SOL ne se termine pas complètement dans l'utilitaire, il est possible les autres sessions SOL ne soient pas disponibles. Pour résoudre ce problème, arrêtez la console de ligne de commande dans l'interface Web sous **Paramètres iDRAC** > **Connectivité** > **Série sur LAN**.

Communication avec l'iDRAC à l'aide d'IPMI sur LAN

Vous devez configurer IPMI sur LAN pour l'iDRAC afin d'activer ou de désactiver les commandes IPMI sur les canaux LAN vers tous les systèmes externes. Si IPMI sur LAN n'est pas configuré, les systèmes externes ne peuvent pas communiquer avec le serveur iDRAC à l'aide des commandes IPMI.

REMARQUE : IPMI prend également en charge le protocole d'adresse IPv6 pour les systèmes d'exploitation Linux.

Configuration d'IPMI sur le LAN à l'aide de 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 RACADM

1. Activer IPMI sur le LAN

```
racadm set iDRAC.IPMILan.Enable 1
```

   REMARQUE : Ce paramètre détermine les commandes IPMI exécutées à l'aide de 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.

```
racadm set iDRAC.IPMILan.PrivLimit <level>
```

Paramètre	Niveau de privilège
<level> = 2	Utilisateur
<level> = 3	Opérateur
<level> = 4	Administrateur

3. Définissez la clé de chiffrement du canal LAN IPMI, si nécessaire.

```
racadm set iDRAC.IPMILan.EncryptionKey <key>
```

Paramètre	Description
<key>	Clé de chiffrement à 20 caractères dans un format hexadécimal valide.

REMARQUE : L'IPMI de l'iDRAC prend en charge le protocole RMCP+. Pour plus d'informations, voir les spécifications IPMI 2.0 sur le site **intel.com**.

Configuration d'IPMI sur LAN en utilisant l'interface Web

Configurez IPMI sur le LAN :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Connectivité**.
   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'iDRAC**.

   Les paramètres IPMI sur le LAN sont définis.

Activation ou désactivation de l'interface distante RACADM

Vous pouvez activer ou désactiver l'interface distante RACADM à l'aide de l'interface Web de l'iDRAC ou de RACADM. Vous pouvez exécuter jusqu'à cinq sessions RACADM distantes en parallèle.

REMARQUE : L'interface distante RACADM est activée par défaut.

Activation ou désactivation de l'interface RACADM distante à l'aide de RACADM

REMARQUE : Il est recommandé d'exécuter ces commandes à l'aide de l'interface RACADM locale ou du firmware RACADM.

Pour désactiver l'interface RACADM distante :

- Pour désactiver l'interface RACADM distante :

```
racadm set iDRAC.Racadm.Enable 0
```

- Pour activer l'interface RACADM distante :

```
racadm set iDRAC.Racadm.Enable 1
```

Activation ou désactivation de l'interface distante RACADM à l'aide de l'interface web

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Services**.
2. Sous **Interface distante RACADM**, sélectionnez l'option souhaitée et cliquez sur **Appliquer**.
   L'interface RACADM distante est activée ou désactivée en fonction de la sélection.

Désactivation de l'interface locale RACADM

L'interface RACADM locale est activée par défaut. Pour la désactiver, voir Désactivation de l'accès pour modifier les paramètres de configuration iDRAC sur un système hôte.

Configuration de Linux pour la console série pendant le démarrage sous RHEL

Les étapes suivantes sont propres à GRUB (Linux GRand Unified Bootloader). Des modifications similaires sont nécessaires en cas d'utilisation d'un chargeur de démarrage différent.

REMARQUE : Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console 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** comme suit :

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
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sda1
# 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.

REMARQUE : Si le chargeur de démarrage ou le système d'exploitation assure la redirection série, comme c'est le cas de GRUB ou Linux, le paramètre BIOS **Redirection After Boot (Redirection après démarrage)** doit être désactivé. Cela évite que plusieurs composants se fassent concurrence pour accéder au port série.

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 This file describes how the INIT process should set up
#the system in a certain run-level.
#Author:Miquel van Smoorenburg
#Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this)
#1 - Single user mode
#2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode
#4 - unused
#5 - X11
#6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
#System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
#Things to run in every runlevel.
ud::once:/sbin/update
ud::once:/sbin/update
#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few
#minutes of power left. Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have power installed and your
#UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
#Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

#Run xdm in runlevel 5
#xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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 : Utilisez 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
```

Configuration du terminal série sous RHEL

Pour configurer le terminal série sous RHEL :

1. Ajouter ou mettre à jour les lignes suivantes de `/etc/default/grub` :

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8"
   ```

   ```
   GRUB_TERMINAL="console serial"
   ```

   ```
   GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1"
   ```

   `GRUB_CMDLINE_LINUX_DEFAULT` applique cette configuration uniquement à l'entrée de menu par défaut ; utilisez `GRUB_CMDLINE_LINUX` pour l'appliquer à toutes les entrées de menu.

   Chaque ligne doit s'afficher une seule fois dans `/etc/default/grub`. Si elle existe, modifiez-la pour éviter de créer un doublon. Par conséquent, une seule ligne `GRUB_CMDLINE_LINUX_DEFAULT` est autorisée.

2. Reconstruisez le fichier de configuration `/boot/grub2/grub.cfg` en exécutant la commande `grub2-mkconfig -o` de la manière suivante :
   - Sur des systèmes du type BIOS :

     ```
     ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
     ```

   - Sur des systèmes du type UEFI :

     ```
     ~]# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
     ```

Pour plus d'informations, consultez le Guide de l'administrateur système RHEL à l'adresse redhat.com.

Contrôle de GRUB depuis une console série

Vous pouvez configurer GRUB pour utiliser la console série au lieu de la console VGA. Cela vous permet d'interrompre le processus de démarrage et de choisir un autre noyau ou d'ajouter des paramètres au noyau, par exemple, pour démarrer en mode utilisateur unique.

Pour que GRUB utilise la console série, commentez l'image d'accueil et ajoutez les options `serial` et `terminal` à `grub.conf` :

```
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
serial --unit=0 --speed=1152001
```

REMARQUE : redémarrez le système pour que les modifications prennent effet.

Schémas cryptographiques SSH pris en charge

Pour communiquer avec iDRAC en utilisant le protocole SSH, iDRAC prend en charge les schémas cryptographiques répertoriés dans le tableau suivant.

Tableau 20. Schémas cryptographiques SSH

Type de schéma	Algorithmes
Cryptographie asymétrique	
Clé publique	• curve25519-sha256 • curve25519-sha256@libssh.org • ssh-rsa • ecdsa-sha2-nistp256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 • diffie-hellman-group14-sha256
Cryptographie symétrique	
Échange de clés	• rsa-sha2-512 • rsa-sha2-256

Tableau 20. Schémas cryptographiques SSH (suite)

Type de schéma	Algorithmes
	• ssh-rsa • ecdsa-sha2-nistp256 • ssh-ed25519 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group-exchange-sha256
Cryptage	• chacha20-poly1305@openssh.com • aes128-ctr • aes192-ctr • aes256-ctr • aes128-gcm@openssh.com • aes256-gcm@openssh.com
MAC	• umac-64@openssh.com • umac-128-etm@openssh.com • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • umac-128@openssh.com • hmac-sha2-256 • hmac-sha2-512
Compression	Aucun

REMARQUE : Si vous activez OpenSSH 7.0 ou version ultérieure, la prise en charge de la clé publique DSA est désactivée. Pour optimiser la sécurité d'iDRAC, Dell vous recommande de ne pas activer la prise en charge de la clé publique DSA.

Utilisation de l'authentification par clé publique pour SSH

L'iDRAC prend en charge l'authentification par clé publique (PKA) via SSH. Il s'agit d'une fonctionnalité sous licence. Lorsque l'authentification par clé publique via SSH est configurée et utilisée correctement, vous devez saisir le nom d'utilisateur lors de la connexion à l'iDRAC. Cela est utile pour configurer des scripts automatisés afin d'exécuter diverses fonctions. Les clés téléchargées doivent être au format RFC 4716 ou OpenSSH. Sinon, vous devez convertir les clés dans ce format.

Dans tous les cas, une paire de clés privée et publique doit être générée sur la station de gestion. La clé publique est chargée sur l'utilisateur local de l'iDRAC, et la clé privée est utilisée par le client SSH pour établir la relation de confiance entre la station de gestion et l'iDRAC.

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 généralement réservé aux utilisateurs membres du groupe d'utilisateurs Administrateur sur l'iDRAC. Il est cependant possible de l'attribuer aussi aux utilisateurs du groupe d'utilisateurs Personnalisé. Un utilisateur détenant ce privilège peut modifier n'importe quelle configuration d'utilisateur, notamment créer ou supprimer tout utilisateur, la gestion de clés SSH des utilisateurs, etc. Pour ces raisons, vous devez attribuer soigneusement ce privilège.

PRÉCAUTION : La possibilité de charger, d'afficher et/ou de supprimer des clés SSH dépend du privilège utilisateur « Configurer les utilisateurs ». Ce privilège permet à un ou plusieurs utilisateurs de configurer la clé SSH d'un autre utilisateur. Vous devez accorder ce privilège avec soin.

Génération de clés publiques pour Linux

Pour utiliser l'application **ssh-keygen** en vue de créer la clé de base, ouvrez une fenêtre de terminal et, à l'invite du shell, saisissez `ssh-keygen -t rsa -b 2048 -C testing`

Où :

- `-t` correspond à **rsa**.
- `-b` spécifie la taille du chiffrement binaire comprise entre 2 048 et 4 096.
- `-C` permet de modifier le commentaire de la clé publique (option facultative).

REMARQUE : Les options sont sensibles à la casse.

Suivez les instructions. Après l'exécution de la commande, chargez le fichier public.

PRÉCAUTION : Les clés générées à partir de la station de gestion Linux à l'aide de ssh-keygen ne sont pas au format 4716. Convertissez les clés au format 4716 à l'aide de `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Ne modifiez pas les autorisations du fichier de clés. La conversion doit être effectuée à l'aide des autorisations par défaut.

REMARQUE : iDRAC ne prend pas en charge le transfert des clés via ssh-agent.

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 RSA comme type de clé.
2. Saisissez le nombre de bits de la clé. Le nombre de bits doit être compris entre 2 048 et 4 096.
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.

Téléversement de clés SSH

Vous pouvez charger jusqu'à quatre clés publiques **par utilisateur** à utiliser via une interface SSH. Avant d'ajouter des clés publiques, veillez à ce que les clés s'affichent correctement si elles sont définies afin de ne pas les écraser par inadvertance.

Lors de l'ajout de nouvelles clés publiques, assurez-vous que les clés existantes ne se trouvent pas à l'index où la nouvelle clé est ajoutée. L'iDRAC n'effectue pas de vérifications pour s'assurer que la ou les clés précédentes sont supprimées avant l'ajout d'une ou plusieurs nouvelles clés. Lorsque vous ajoutez une nouvelle clé, vous pouvez l'utiliser à condition que l'interface SSH soit activée.

Téléversement des clés SSH à l'aide de l'interface Web

Pour téléverser des clés SSH :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Utilisateurs locaux**.
   La page **Utilisateurs locaux** s'affiche.
2. Dans la colonne **ID 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 fichier de clé.
   - Copiez le contenu du fichier de clé dans zone de texte.

   Pour en savoir plus, voir l'Aide en ligne de l'iDRAC.
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 RACADM locale : `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- À partir de l'interface RACADM distante ou SSH : `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

Par exemple, pour téléverser une clé valide vers l'ID utilisateur iDRAC 2 dans l'espace de la première clé à l'aide d'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 ssh/série.

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.

Suppression des clés SSH en utilisant l'interface RACADM

Pour supprimer les clés SSH, exécutez les commandes suivantes :

- Clé spécifique : `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- Toutes les clés : `racadm sshpkauth -i <2 to 16> -d -k all`

Suppression de clés SSH à l'aide de l'interface Web

Pour supprimer des clés SSH :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs**.
   La page **Utilisateurs locaux** s'affiche.
2. Dans la colonne **ID**, sélectionnez un numéro d'ID utilisateur, puis cliquez sur **Modifier**.
   La page **Modifier un utilisateur** s'affiche.
3. Sous **Configurations de clés SSH**, sélectionnez une clé SSH, puis cliquez sur **Modifier**.
   La page **Clé SSH** affiche les détails du champ **Modifier depuis**.
4. Sélectionnez **Supprimer** en regard des clés à supprimer, puis cliquez sur **Appliquer**.
   Les clés sélectionnées sont supprimées.

Affichage des clés SSH

Vous pouvez afficher les clés téléversées vers iDRAC.

Affichage des clés SSH à l'aide de l'interface Web

Pour afficher les clés SSH :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs**.
   La page **Utilisateurs locaux** s'affiche.
2. Dans la colonne **ID utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configurations de clés SSH**, sélectionnez **Afficher/Supprimer une ou des clés SSH** et cliquez sur **Suivant**.
   La page **Afficher/Supprimer une ou des clés SSH** s'affiche avec les détails des clés.

11

Comptes d'utilisateur et rôles d'utilisateur

Vous pouvez créer des rôles d'utilisateur avec des privilèges spécifiques à l'aide de l'iDRAC pour gérer votre système et maintenir la sécurité du système. Par défaut, l'iDRAC est configuré avec un rôle d'administrateur local. Par défaut, le nom d'utilisateur et le mot de passe de l'iDRAC sont fournis avec le badge du système. Pour plus d'informations, voir la documentation du serveur.

En tant qu'administrateur, vous pouvez créer des rôles d'utilisateur avec les privilèges associés. Vous pouvez créer des comptes utilisateur et leur attribuer les rôles nouvellement créés ou des rôles existants **Administrateur**, **Opérateur**, **Lecture seule** dans l'iDRAC. Vous pouvez configurer des utilisateurs locaux ou utilisez des services d'annuaire (Microsoft Active Directory ou LDAP, par exemple) pour configurer des comptes utilisateur. L'utilisation d'un service de répertoire fournit un site central de gestion des comptes d'utilisateur autorisés.

Sujets :

Rôles et privilèges utilisateurs iDRAC

Les rôles iDRAC par défaut sont **Administrateur**, **Opérateur**et **Lecture seule**. Ces rôles disposent de privilèges d'utilisateur spécifiques.

Le tableau suivant répertorie les noms de rôle iDRAC par défaut :

Tableau 21. Rôles iDRAC

Rôles	Privilèges
Administrateur	Se connecter à l'iDRAC, configurer l'iDRAC, configurer les utilisateurs, effacer les journaux, configurer le système, accéder à la console virtuelle, accéder au média virtuel, tester les alertes, exécuter les commandes de débogage.
Opérateur	Se connecter à l'iDRAC, Configurer l'iDRAC, Effacer les journaux, Configurer le système, Accéder au média virtuel, Tester les alertes et Exécuter les commandes de débogage.
LectureSeule	Connectez-vous à iDRAC.

Le tableau suivant décrit les privilèges d'utilisateur :

Tableau 22. Privilèges utilisateur iDRAC

Privilèges	Description
Connexion à l'iDRAC.	Permet aux utilisateurs de se connecter à l'iDRAC.
Configurer iDRAC.	Permet aux utilisateurs de configurer l'iDRAC. Avec ce privilège, un utilisateur peut également configurer la gestion de l'alimentation, la console virtuelle, le média virtuel, les licences, les paramètres du système, les appareils de stockage, les paramètres BIOS, SCP et ainsi de suite.
REMARQUE : Le rôle d'administrateur remplace tous les privilèges des autres composants, tels que le mot de passe de configuration du BIOS.	
Configurer des utilisateurs	Permet aux utilisateurs de créer des comptes utilisateur.
Effacer des journaux	Permet aux utilisateurs d'effacer uniquement les journaux des événements système (SEL).

Tableau 22. Privilèges utilisateur iDRAC (suite)

Privilèges	Description
Configurer le système	Permet aux utilisateurs de redémarrer le système hôte.
Accéder à la console virtuelle	Permet aux utilisateurs d'exécuter la console virtuelle.
Accéder à Média Virtuel	Permet aux utilisateurs d'exécuter et d'utiliser Média Virtuel.
Alertes de test	Permet aux utilisateurs de tester les alertes par e-mail, les traps SNMP et d'autres notifications d'alerte configurées.
Exécuter les commandes de débogage	Permet aux utilisateurs d'exécuter des commandes de diagnostic.

Caractères recommandés pour les noms d'utilisateur et mots de passe

Cette section fournit des détails sur les caractères recommandés lors de la création et de l'usage des noms d'utilisateur et mots de passe.

REMARQUE : Le mot de passe doit contenir une majuscule et une lettre minuscule, un chiffre et un caractère spécial.

Utilisez les caractères suivants lors de la création des noms d'utilisateur et mots de passe :

Tableau 23. Caractères recommandés pour les noms d'utilisateur

Caractères	Longueur
• 0 à 9 • A-Z • a-z • - ! # $ % & ( ) * ; ? [\ ] ^ _ ` { | } ~ + < = >	1–16

Tableau 24. Caractères recommandés pour les mots de passe

Caractères	Versions iDRAC10	Longueur
• 0 à 9 • A-Z • a-z • ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1.10.17.00 et versions ultérieures	1–127

REMARQUE : Vous pouvez créer des noms d'utilisateur et des mots de passe qui comprennent d'autres caractères. Toutefois, pour garantir la compatibilité avec toutes les interfaces, Dell recommande d'utiliser uniquement les caractères répertoriés ici.

REMARQUE : Les caractères autorisés dans les noms d'utilisateur et les mots de passe pour les partages réseau sont déterminés par le type de partage réseau. L'iDRAC prend en charge les caractères valides pour les informations d'identification de partage réseau, telles que définies par le type de partage, à l'exception des caractères <, > et , (virgule).

REMARQUE : Pour améliorer la sécurité, il est recommandé d'utiliser des mots de passe complexes qui comportent au moins huit caractères, y compris des minuscules, des majuscules, des chiffres et des caractères spéciaux. Il est également recommandé de changer régulièrement ces mots de passe, si possible.

Création de rôles d'utilisateur

Vous pouvez créer des rôles d'utilisateur avec les privilèges requis afin de pouvoir déléguer efficacement les tâches aux utilisateurs. Seuls les utilisateurs disposant du rôle d'administrateur peuvent créer des rôles d'utilisateur.

1. Accédez à **Paramètres IDRAC** > **Utilisateurs** > **Utilisateurs locaux** > **Rôles d'utilisateurs**.
2. Cliquez sur **+Ajouter**.

La boîte de dialogue **Ajouter un nouveau rôle** s'affiche.

3. Sélectionnez l'**ID utilisateur**.
4. Saisissez le **Nom du rôle d'utilisateur**.
5. Sélectionnez **Privilèges des utilisateurs**.
6. Cliquez sur **Enregistrer**.
   Le rôle d'utilisateur est répertorié dans la liste des **rôles d'utilisateur**.

Configuration des utilisateurs locaux

Vous pouvez configurer jusqu'à 32 utilisateurs locaux dans l'iDRAC avec des rôles d'utilisateur spécifiques. Avant de créer un utilisateur iDRAC, vérifiez s'il existe des utilisateurs actuels. Vous pouvez définir des noms d'utilisateurs, des mots de passe et des rôles avec des privilèges pour ces utilisateurs. Il est possible de modifier les noms d'utilisateur et les mots de passe à l'aide de n'importe quelle interface iDRAC sécurisée (à savoir, l'interface Web, RACADM ou Redfish).

Créer des utilisateurs locaux à l'aide de l'interface utilisateur iDRAC

Vous pouvez ajouter des utilisateurs et attribuer des rôles spécifiques aux utilisateurs en fonction des tâches qui leur sont attribuées.

REMARQUE : Vous ne pouvez créer des utilisateurs que si le rôle d'utilisateur qui vous est attribué dispose du privilège **Configurer les utilisateurs**.

1. Dans l'interface utilisateur iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs locaux** > **Vue d'ensemble**.
   Les utilisateurs locaux sont répertoriés.
2. Cliquez sur **+Ajouter**.
   La boîte de dialogue **Ajouter un nouvel utilisateur** s'affiche.
3. Sélectionnez l'**ID**.
4. Saisissez les champs **Nom d'utilisateur**, **Mot de passe** et **Confirmer le mot de passe**.
5. Sélectionnez le **rôle utilisateur**.
   Les **privilèges utilisateur** correspondants s'affichent.
6. Cliquez sur **Enregistrer**.
   Le nom d'utilisateur s'affiche dans la liste.

Configuration des utilisateurs locaux à l'aide de 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 iDRAC à l'aide de RACADM.

Pour configurer plusieurs utilisateurs iDRAC avec des paramètres de configuration identiques, procédez comme suit :

- Inspirez-vous des exemples RACADM indiqués dans cette section pour créer un fichier de commandes RACADM, puis exécutez ce fichier sur chaque système géré.
- Créez le fichier de configuration iDRAC et exécutez la commande `racadm set` sur chaque système géré en utilisant le même fichier de configuration.

Si vous configurez un nouveau contrôleur iDRAC ou si vous avez utilisé la commande `racadm racresetcfg`, vérifiez le nom d'utilisateur et le mot de passe par défaut de l'iDRAC sur le badge du système. La commande `racadm racresetcfg` rétablit les valeurs par défaut de l'iDRAC.

REMARQUE : Si SEKM est activé sur le serveur, désactivez-le à l'aide de la commande `racadm sekm disable` avant d'utiliser cette commande. Cela peut empêcher le verrouillage de tous les appareils de stockage sécurisés par l'iDRAC si les paramètres SEKM sont effacés de l'iDRAC en exécutant cette commande.

REMARQUE : Des utilisateurs peuvent être activés et désactivés au fil du temps. De ce fait, un utilisateur peut avoir sur chaque iDRAC un numéro d'index différent.

Pour vérifier si un utilisateur existe, tapez la commande suivante une fois pour chaque index (de 1 à 16) :

```
racadm get iDRAC.Users.<index>.UserName
```

Plusieurs paramètres et ID d'objet sont affichés avec leurs valeurs actuelles. Le champ clé est `iDRAC.Users.UserName=`. Si un nom d'utilisateur s'affiche après =, c'est que ce numéro d'index est pris.

REMARQUE : Vous pouvez utiliser

```
racadm get -f <myfile.cfg>
```

et visualiser ou modifier le fichier

```
myfile.cfg
```

, qui comprend tous les paramètres de configuration iDRAC.

Pour activer l'authentification SNMP v3 d'un utilisateur, utilisez les objets **SNMPv3AuthenticationType**, **SNMPv3Enable** et **SNMPv3PrivacyType**. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Si vous utilisez le fichier de configuration de serveur pour configurer des utilisateurs, utilisez les attributs **AuthenticationProtocol**, **ProtocolEnable** et **PrivacyProtocol** pour activer l'authentification SNMPv3.

Ajout d'un utilisateur iDRAC à l'aide de RACADM

1. Définissez l'index et le nom d'utilisateur.

   ```
   racadm set idrac.users.<index>.username <user_name>
   ```

Paramètre	Description
<index>	Index unique de l'utilisateur
<user_name>	Nom d'utilisateur

2. Définissez le mot de passe.

   ```
   racadm set idrac.users.<index>.password <password>
   ```

3. Définissez les privilèges d'utilisateur.

   Pour en savoir plus, voir le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

4. Activez l'utilisateur.

   ```
   racadm set idrac.users.<index>.enable 1
   ```

Pour vérifier, utilisez la commande suivante :

```
racadm get idrac.users.<index>
```

Pour en savoir plus, voir le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Activation d'un utilisateur iDRAC avec des droits

Pour activer un utilisateur avec des droits (droit basé sur un rôle) :

1. Recherchez un index d'utilisateurs disponible.

   ```
   racadm get iDRAC.Users <index>
   ```

2. Tapez les commandes suivantes avec les nouveaux nom d'utilisateur et mot de passe.

   ```
   racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
   ```

REMARQUE : La valeur de privilège par défaut est 0, qui indique qu'aucun privilège n'est activé pour l'utilisateur. Pour obtenir une liste des valeurs de masque binaire valides correspondant à des privilèges d'utilisateur spécifiques, voir le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Configuration des utilisateurs d'Active Directory

Si votre société utilise le logiciel Microsoft Active Directory, vous pouvez le configurer pour fournir l'accès à iDRAC, ce qui permet d'ajouter des privilèges iDRAC aux utilisateurs existants et de les contrôler dans le service de répertoire. Il s'agit d'une fonctionnalité sous licence.

Vous pouvez configurer l'authentification utilisateur via Active Directory pour la connexion à iDRAC. Vous pouvez également fournir une autorité basée sur le rôle, ce qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur.

REMARQUE : StartTLS sur le port 389 est pris en charge. Par défaut, LDAPS sur le port 636 est configuré. Le protocole de connexion peut être reconfiguré sur StartTLS à l'aide de la commande Redfish ou RACADM `racadm set iDRAC.ActiveDirectory.Connection StartTLS`.

Exigences d'utilisation de l'authentification Active Directory pour l'iDRAC

Pour utiliser la fonction d'authentification Active Directory d'iDRAC, vérifiez que vous avez :

- Déployé une infrastructure Active Directory. Pour plus d'informations, voir le site Web de Microsoft.
- PKI intégrée dans l'infrastructure Active Directory. L'iDRAC utilise le mécanisme PKI (public Key infrastructure) standard pour s'authentifier en toute sécurité dans Active Directory. Pour plus d'informations, voir le site Web de Microsoft.
- Activé SSL (Secure Socket Layer) dans tous les contrôleurs de domaine auxquels iDRAC se connecte pour l'authentification dans tous les contrôleurs de domaine.

Activation de SSL sur un contrôleur de domaine

Lorsque l'iDRAC authentifie les utilisateurs avec un contrôleur de domaine Active Directory, il démarre une session SSL avec ce 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 chargé dans l'iDRAC. Pour que l'iDRAC puisse s'authentifier auprès d'un contrôleur de domaine, qu'il s'agisse du contrôleur de domaine racine ou enfant, ce contrôleur de domaine doit disposer d'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 iDRAC ;
3. importer le certificat SSL du micrologiciel d'iDRAC.

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**, puis sur **Terminer**. Le certificat SSL est installé.

Exportation d'un certificat CA racine de contrôleur de domaine vers l'iDRAC

Pour exporter le certificat CA racine du contrôleur de domaine vers iDRAC :

1. Localisez le contrôleur de domaine qui exécute le service CA d'entreprise Microsoft.
2. Cliquez sur **Démarrer** > **Exécuter**.
3. Saisissez `mmc` et cliquez sur **OK**.
4. Dans la fenêtre **Console 1** (MMC), cliquez sur **Fichier (**ou sur **Console)** 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 **Console 1**, accédez au dossier **Certificats Personnel Certificats**.
10. Recherchez le certificat CA racine et cliquez dessus avec le bouton droit 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 iDRAC le certificat que vous avez enregistré au cours de l'étape 13.

Importation du certificat SSL du micrologiciel d'iDRAC

Le certificat SSL iDRAC est le même que celui du serveur Web iDRAC. Tous les contrôleurs iDRAC sont équipés d'un certificat auto-signé par défaut.

Si le serveur Active Directory est configuré pour authentifier le client pendant la phase d'initialisation d'une session SSL, vous devez importer le certificat de serveur iDRAC sur le contrôleur de domaine Active Directory. Cette étape supplémentaire n'est pas requise si Active Directory n'effectue pas d'authentification client pendant la phase d'initialisation d'une session SSL.

REMARQUE : Si le certificat SSL du micrologiciel d'iDRAC 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 iDRAC vers toutes les listes de certificats de confiance du contrôleur de domaine :

1. Téléchargez le certificat SSL iDRAC à l'aide de la commande RACADM suivante :

   ```
   racadm sslcertdownload -t 1 -f <RAC SSL certificate>
   ```

2. Sur le contrôleur de domaine, ouvrez une fenêtre **MMC Console (Console MMC)** et sélectionnez **Certificates (Certificats)** > **Trusted Root Certification Authorities (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'iDRAC dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

   Si vous avez installé votre propre certificat, assurez-vous que l'autorité de certification qui le signe figure sur la liste **Trusted Root Certification Authority (Autorité de certification racine de confiance)**. Si ce n'est pas le cas, vous devez l'installer sur tous vos 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 **Finish (Terminer)**, puis sur **OK**. Le certificat SSL du micrologiciel iDRAC est importé vers toutes les listes de certificats de confiance du contrôleur de domaine.

Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur iDRAC en utilisant deux méthodes :

- La solution de **schéma standard** qui utilise uniquement des objets du groupe Active Directory.
- La solution de **schéma étendu**, qui dispose d'objets Active Directory personnalisés. Tous les objets de contrôle d'accès sont conservés dans Active Directory. Cette solution offre une flexibilité maximale pour configurer l'accès des utilisateurs sur différents contrôleurs iDRAC avec différents niveaux de privilèges.

Présentation d'Active Directory avec le schéma standard

Comme le montre la figure ci-dessous, l'utilisation du schéma standard pour l'intégration d'Active Directory exige des opérations de configuration à la fois dans Active Directory et dans CMC.

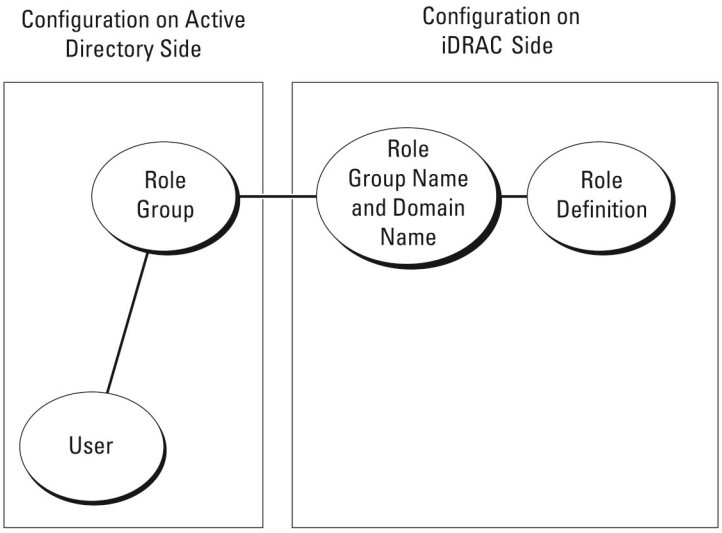


Figure 1. Configuration d'iDRAC avec le schéma standard d'Active Directory

Dans Active Directory, un objet de groupe standard est utilisé en tant que groupe de rôles. Un utilisateur disposant d'un accès iDRAC est membre du groupe de rôles. Pour permettre à cet utilisateur d'accéder à un iDRAC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur l'iDRAC spécifique. Le rôle et le niveau de privilège sont définis sur chaque iDRAC et non pas dans Active Directory. Vous pouvez configurer jusqu'à 15 groupes de rôles dans chaque iDRAC. Le numéro de référence du tableau affiche les privilèges du groupe de rôles par défaut.

Tableau 25. 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, Accéder 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	0x0000001f3
Groupe de rôles 3	Aucun	Connexion à l'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 le RACADM.

Scénarios impliquant un seul domaine et scénarios 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 l'iDRAC. Dans ce scénario impliquant un seul domaine, n'importe quel type de groupe est pris en charge.

Si tous les utilisateurs de connexion et groupes de rôles, ou l'un des groupes imbriqués, sont issus de plusieurs domaines, les adresses des serveurs du catalogue global doivent être configurées sur l'iDRAC. Dans ce scénario impliquant plusieurs domaines, tous les groupes de rôles et les groupes imbriqués, le cas échéant, doivent être de type Groupe universel.

Configuration d'Active Directory avec le schéma standard

Avant de configurer le schéma standard d'Active Directory, assurez-vous que :

- Vous disposez de la licence iDRAC Entreprise ou Datacenter.
- La configuration est effectuée sur un serveur qui est utilisé en tant que contrôleur de domaine.
- La date, l'heure et le fuseau horaire sur le serveur sont corrects.
- Les paramètres réseau de l'iDRAC sont configurés (ou, dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC > Connectivité > Réseau > Paramètres communs** pour configurer les paramètres réseau).

Pour configurer l'iDRAC pour l'accès à une connexion Active Directory :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le snap-in Utilisateurs et ordinateurs Active Directory.
2. Créez les groupes et les utilisateurs iDRAC.
3. Définissez le nom du groupe, le nom de domaine et les privilèges de rôle dans l'iDRAC en utilisant l'interface Web ou RACADM de l'iDRAC.

Configuration d'Active Directory avec le schéma standard à l'aide de RACADM

1. Utilisez les commandes suivantes :

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ADGroup.Name <common name of the role group>
racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
racadm set iDRAC.ADGroup.Privilege <Bit-mask value for specific RoleGroup permissions>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP address
of the domain controller>
```

- Entrez le nom de domaine complet qualifié (FQDN) du contrôleur de domaine et non celui du domaine. Par exemple, saisissez `servername.dell.com` au lieu de `dell.com`.
- Pour les valeurs de masque binaire des autorisations de Groupe de rôles spécifiques, voir Privilèges de groupe de rôles par défaut.
- Vous devez fournir au moins l'une des trois adresses de contrôleur de domaine. L'iDRAC tente de se connecter à chacune des adresses configurées l'une après l'autre jusqu'à établir une connexion réussie. Si le schéma standard est sélectionné, il s'agira des adresses des contrôleurs de domaine dans lesquelles les comptes d'utilisateur et les groupes de rôles sont situés.
- Le serveur de catalogue global est requis uniquement 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.
- Si la validation de certificat est activée, le nom de domaine complet ou l'adresse IP que vous spécifiez dans ce champ doivent correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine.
- Pour désactiver la validation de certificat durant l'établissement d'une liaison SSL, utilisez la commande suivante :

```
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 l'établissement d'une liaison SSL (facultatif), utilisez la commande suivante :

```
racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
```

Dans ce cas, vous devez téléverser le certificat d'autorité de certification en utilisant la commande suivante :

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

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. Assurez-vous que le DNS est correctement configuré sous **Overview (Présentation)** > **iDRAC Settings (Paramètres iDRAC)** > **Network (Réseau)**.

L'utilisation de la commande RACADM suivante peut être facultative.

```
racadm sslcertdownload -t 1 -f <RAC SSL certificate>
```

2. Si DHCP est activé sur l'iDRAC et que vous voulez utiliser le DNS fourni par le serveur DHCP, entrez la commande suivante :

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3. Si DHCP est désactivé sur iDRAC ou que vous voulez entrer manuellement l'adresse IP DNS, entrez la commande RACADM suivante :

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4. Si vous souhaitez configurer une liste de domaines d'utilisateurs pour n'avoir à entrer que le nom d'utilisateur lors de la connexion à l'interface web, entrez la commande suivante :

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

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

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC

REMARQUE : Pour plus d'informations sur les champs, voir l'**aide en ligne d'iDRAC**.

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Services d'annuaire**.
   La page **Services d'annuaire** s'affiche.
2. Sélectionnez l'option **Microsoft Active Directory**, puis cliquez sur **Modifier**.
   La page **Configuration et gestion d'Active Directory** s'affiche.
3. Cliquez sur **Configurer Active Directory**.
   La page **Configuration et gestion d'Active Directory - Étape 1 sur 4** s'affiche.
4. 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). Pour cela, vous devez spécifier les contrôleurs de domaine et le FQDN du catalogue global. Consultez les étapes suivantes. Par conséquent, le DNS doit être correctement configuré dans les paramètres réseau.
5. Cliquez sur **Next**.

   La page **Configuration et gestion d'Active Directory -Étape 2 sur 4** s'affiche.

6. Activez Active Directory et définissez les informations d'emplacement des serveurs et des comptes d'utilisateur Active Directory. Spécifiez en outre le délai pendant lequel l'iDRAC doit attendre les réponses d'Active Directory lors de la connexion à l'iDRAC.

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. Assurez-vous que le DNS est correctement configuré sous **Paramètres iDRAC** > **Réseau**.

7. Cliquez sur **Next**. La page **Configuration et gestion d'Active Directory -Étape 3 sur 4** s'affiche.
8. Sélectionnez **Schéma standard**, puis cliquez sur Suivant.
   La page **Configuration et gestion d'Active Directory - Étape 4a sur 4** s'affiche.
9. Entrez l'emplacement du ou des services de catalogue global Active Directory et définissez les groupes de privilèges utilisés pour autoriser les utilisateurs.
10. 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.
11. 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.
12. Cliquez sur **Terminer**. Les paramètres Active Directory pour le schéma standard sont définis.

Présentation d'Active Directory avec schéma étendu

Pour utiliser la solution de schéma étendu, vous devez disposer de l'extension de schéma Active Directory.

Les pratiques d'excellence pour le schéma étendu

Le schéma étendu utilise des objets Association Dell pour rejoindre l'iDRAC et obtenir des autorisations. Cela vous permet d'utiliser l'iDRAC en fonction des autorisations globales accordées. La liste de contrôle d'accès (ACL) par défaut des objets Association Dell permet aux administrateurs autonomes et aux administrateurs de domaine de gérer les autorisations et le champ d'application des objets iDRAC.

Par défaut, les objets Association Dell n'héritent pas de toutes les autorisations des objets Active Directory parents. Si vous activez l'héritage pour l'objet Association Dell, les autorisations héritées pour cet objet Association sont accordées aux utilisateurs et groupes sélectionnés. Cela peut entraîner l'octroi involontaire de privilèges à l'iDRAC.

Pour utiliser le schéma étendu en toute sécurité, Dell recommande de ne pas activer l'héritage sur les objets Association de Dell dans le cadre de l'implémentation du schéma étendu.

Extensions de schéma Active Directory

Les données Active Directory se trouvent dans une base de données distribuée d'**attributs** et de **classes**. Le schéma Active Directory inclut les règles qui déterminent le type de données qu'il est possible d'ajouter ou d'inclure dans la base de données. La classe utilisateur est un exemple de **classe** stockée dans la base de données. Le prénom, le nom et le numéro de téléphone de l'utilisateur sont des exemples d'attributs de classe. Vous pouvez étendre la base de données Active Directory en ajoutant vos propres **attributs** et **classes** uniques pour des besoins spécifiques. Dell a étendu le schéma pour inclure les modifications nécessaires à la prise en charge de l'authentification et de l'autorisation de la gestion à distance à l'aide d'Active Directory.

Vous devez définir chaque **attribut** ou **classe** ajouté(e) à un schéma Active Directory existant à un ID unique. Pour conserver des ID uniques dans l'ensemble du secteur, Microsoft gère une base de données d'ID d'objets (OID) Active Directory afin que, lorsque les sociétés ajoutent des extensions au schéma, ces extensions soient uniques et n'entrent pas en conflit les unes avec les autres. Pour étendre le schéma dans Active Directory de Microsoft, Dell a reçu des OID uniques, des extensions de nom uniques et des ID d'attribut liés de manière unique pour les attributs et classes ajoutés au service d'annuaire :

- L'extension est : `dell`
- L'OID de base est : `1.2.840.113556.1.8000.1280`
- La plage LinkID RAC est : `12070 to 12079`

Présentation des extensions de schéma d'iDRAC

Dell a étendu le schéma pour inclure les propriétés **Association**, **Appareil** et **Privilège**. La propriété **Association** sert à lier les utilisateurs ou les groupes disposant d'un ensemble spécifique de privilèges à un ou plusieurs appareils iDRAC. Ce modèle offre à l'administrateur une flexibilité maximale sur les différentes combinaisons d'utilisateurs, de privilèges iDRAC et d'appareils iDRAC sur le réseau sans trop de complexité.

Pour chaque appareil iDRAC physique du réseau que vous souhaitez intégrer à Active Directory à des fins d'authentification et d'autorisation, créez au moins un objet Association et un objet Appareil iDRAC. Vous pouvez créer plusieurs objets Association, et lier chacun d'entre eux à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Appareil iDRAC que nécessaire. Les utilisateurs et les groupes d'utilisateurs iDRAC peuvent être membres de n'importe quel domaine de l'entreprise.

Toutefois, chaque objet Association peut être lié (ou peut lier des utilisateurs, des groupes d'utilisateurs ou des objets Appareil iDRAC) à un seul objet Privilège. Cet exemple permet à un administrateur de contrôler les privilèges de chaque utilisateur sur des appareils iDRAC spécifiques.

L'objet Appareil iDRAC correspond au lien vers le firmware de l'iDRAC pour interroger Active Directory à des fins d'authentification et d'autorisation. Lors de l'ajout de l'iDRAC au réseau, l'administrateur doit configurer l'iDRAC et son objet Appareil avec son nom Active Directory de façon à ce que les utilisateurs puissent procéder aux opérations d'authentification et d'autorisation via Active Directory. En outre, l'administrateur doit ajouter l'iDRAC 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.

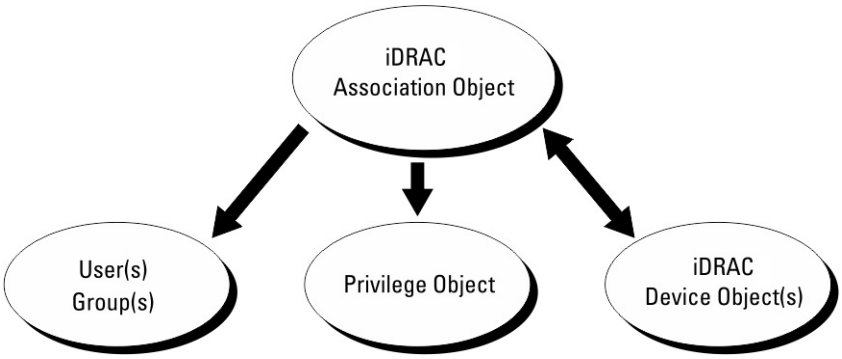


Figure 2. Configuration type pour les objets active directory

Vous pouvez créer un nombre illimité ou réduit d'objets Association. Cependant, vous devez créer au moins un objet Association et devez disposer d'un objet Appareil iDRAC pour chaque appareil iDRAC du réseau à intégrer à Active Directory pour l'authentification et l'autorisation avec l'iDRAC.

L'objet Association permet de créer un nombre illimité ou réduit d'utilisateurs et de groupes ainsi que d'objets Appareil iDRAC. Toutefois, l'objet Association n'inclut qu'un seul objet Privilège par objet Association. L'objet Association connecte les utilisateurs disposant de privilèges sur les appareils iDRAC.

L'extension Dell du composant logiciel enfichable ADUC MMC permet uniquement d'associer l'objet Privilège et les objets iDRAC du même domaine à l'objet Association. L'extension Dell ne permet pas d'ajouter un groupe ou un objet iDRAC d'autres domaines en tant que membre produit de l'objet Association.

Lors de l'ajout de groupes de type Universel à partir de domaines distincts, créez un objet Association avec un champ d'application Universel. Les objets Association créés par défaut par l'utilitaire Schema Extender de Dell sont des groupes locaux de domaine et ne fonctionnent pas avec les groupes de type Universel d'autres domaines.

Il est possible d'ajouter des utilisateurs, des groupes d'utilisateurs ou des groupes d'utilisateurs imbriqués de n'importe quel domaine à l'objet Association. Les solutions de schéma étendu prennent en charge tous les types de groupes d'utilisateurs et tous les groupes d'utilisateurs imbriqués 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 à partir de différents objets de privilège associés au même utilisateur via différents objets Association. En d'autres termes, l'authentification du schéma étendu accumule les privilèges pour permettre à l'utilisateur de disposer de tous les privilèges attribués correspondant aux différents objets de privilège associés au même utilisateur.

L'illustration suivante montre un exemple d'accumulation de privilèges à l'aide du schéma étendu.

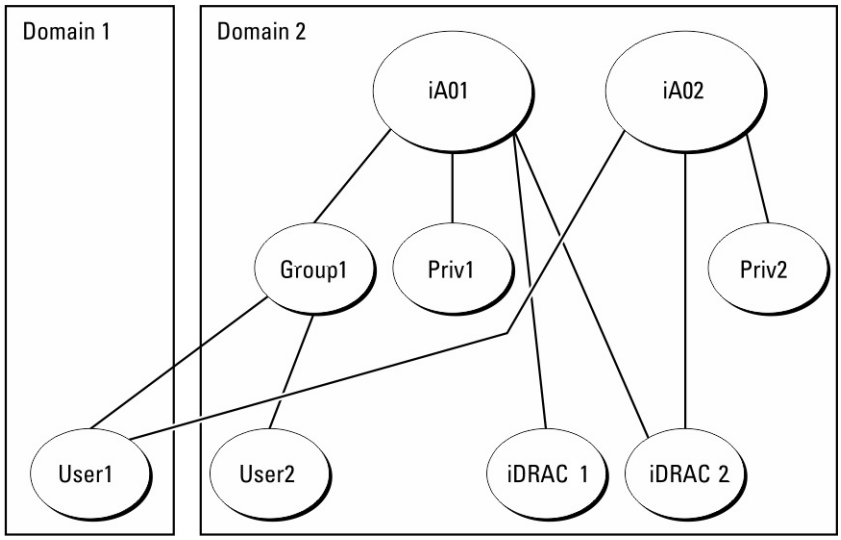


Figure 3. Accumulation de privilèges pour un utilisateur

Cette figure illustre deux objets Association : A01 et A02. L'utilisateur 1 est associé à l'iDRAC 2 via les deux objets Association.

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 à la fois des privilèges Priv1 et Priv2 sur l'iDRAC 2. L'utilisateur 1 dispose des privilèges Priv1 sur l'iDRAC 1 uniquement. L'utilisateur 2 dispose des privilèges Priv1 sur l'iDRAC 1 et l'iDRAC 2. En outre, cette illustration montre que l'utilisateur 1 peut se trouver dans un autre domaine et peut être membre d'un groupe.

Configuration du schéma étendu Active Directory

Pour configurer Active Directory pour qu'il accède à iDRAC :

1. Développez le schéma d'Active Directory.
2. Développez le snap-in Utilisateurs et ordinateurs Active Directory.
3. Ajoutez des utilisateurs iDRAC et leurs privilèges à Active Directory.
4. Configurez les propriétés Active Directory iDRAC à l'aide de l'interface Web ou RACADM d'iDRAC.

Extension du schéma Active Directory

L'extension de votre schéma Active Directory ajoute une unité organisationnelle Dell, des classes et attributs de schéma, ainsi que des exemples de privilèges et d'objets d'association au schéma Active Directory. Avant d'étendre le schéma, assurez-vous de disposer des privilèges Administrateur de schéma sur le propriétaire de rôle d'opération à maître unique flottant (FSMO) de maître de schéma de la forêt de domaines.

REMARQUE : L'extension de schéma de ce produit est différente des générations précédentes. Le schéma précédent 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 organisationnelle 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 garantir le bon fonctionnement de l'utilitaire Dell Schema Extender, ne modifiez pas le nom de ce fichier.

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

   Le schéma est étendu. Pour vérifier l'extension de schéma, utilisez MMC et le snap-in de schéma Active Directory pour vérifier que les classes et attribues existent. Voir la documentation Microsoft pour en savoir plus sur MMC et le snap-in de schéma Active Directory.

Classes et attributs

Tableau 26. Définitions de classe pour les classes ajoutées au schéma Active Directory

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

Tableau 27. DelliDRACdevice class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Représente le périphérique iDRAC Dell. L'iDRAC doit être configuré en tant que delliDRACDevice dans Active Directory. Cette configuration permet à l'iDRAC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 28. delliDRACAssociationObject Class

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

Tableau 29. dellRAC4Privileges Class

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

Tableau 30. 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
Attributs	dellRAC4Privileges

Tableau 31. dellProduct class

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 32. Liste des attributs ajoutés au schéma Active Directory

Nom/Description de l'attribut	OID attribué/IdD d'objet de syntaxe	Valeur unique
dellPrivilegeMember : liste des objets dellPrivilege qui appartiennent à cet attribut.	• 1.2.840.113556.1.8000.1280.1.1.2.1 • Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers : liste des objets dellRacDevice et DelliDRACDevice qui appartiennent à ce rôle. Cet attribut est le lien vers l'avant qui correspond au lien vers l'arrière dellAssociationMembers. ID de lien : 12070	• 1.2.840.113556.1.8000.1280.1.1.2.2 • Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser : TRUE si l'utilisateur possède des droits de connexion sur l'appareil.	• 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 possède des droits de configuration de la carte sur l'appareil.	• 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

Tableau 32. Liste des attributs ajoutés au schéma Active Directory (suite)

Nom/Description de l'attribut	OID attribué/IdD d'objet de syntaxe	Valeur unique
dellIsUserConfigAdmin : TRUE si l'utilisateur possède des droits de configuration d'utilisateur sur l'appareil.	• 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 possède des droits d'effacement de journal sur l'appareil.	• 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 possède des droits de réinitialisation du serveur sur l'appareil.	• 1.2.840.113556.1.8000.1280.1.1.2.7 • Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser : TRUE si l'utilisateur possède des droits de console virtuelle sur l'appareil.	• 1.2.840.113556.1.8000.1280.1.1.2.8 • Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser : TRUE si l'utilisateur possède des droits de média virtuel sur l'appareil.	• 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 possède des droits d'utilisateur d'alertes de test sur l'appareil.	• 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 possède des droits d'administrateur de commandes de débogage sur l'appareil.	• 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 actuelle du schéma est utilisée pour mettre le schéma à jour.	• 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 vers l'arrière correspondant au lien vers l'avant 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 objets dellAssociationObjectMembers qui appartiennent à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut lié dellProductMembers. ID de lien : 12071	• 1.2.840.113556.1.8000.1280.1.1.2.14 • Nom distingué (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 Active Directory

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

Lorsque vous installez le logiciel de gestion des systèmes à l'aide du DVD **Dell Systems Management Tools and Documentation**, vous pouvez étendre le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** au cours du processus d'installation. Voir le Guide d'installation rapide de Dell OpenManage Software pour obtenir des instructions supplémentaires sur l'installation du logiciel de gestion des systèmes. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du snap-in se trouve à l'emplacement suivant :

<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 iDRAC 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 iDRAC en créant des objets Appareil, Association et Privilège. Pour ajouter chaque objet, procédez comme suit :

- Créez un objet Périphérique iDRAC.
- Créez un objet Privilège.
- Créez un objet Association.
- Ajoutez des objets à un objet Association.

Création d'un objet Périphérique iDRAC

Pour créer un objet Périphérique iDRAC :

1. Dans la fenêtre **Racine de la console** MMC, cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** > **Dell Remote Management Object Advanced**.
   La fenêtre **Nouvel objet** s'affiche.
3. Entrez le nom du nouvel objet. Le nom doit être identique au nom iDRAC que vous saisissez lors de la configuration des propriétés Active Directory à l'aide de l'interface Web de l'iDRAC.
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 iDRAC provient d'un groupe et son étendue est définie sur Domaine local.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** > **Dell Remote Management Object Advanced**.
   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.

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** > **Modification ADSI**. La fenêtre **Modification 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. Saisissez `Authenticated Users`, cliquez sur **Vérifier les noms**, puis sur **OK**. Les utilisateurs authentifiés sont ajoutés à la liste **Noms des groupes et des 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 iDRAC ou des groupes de périphériques iDRAC.

Vous pouvez ajouter des groupes d'utilisateurs et des périphériques iDRAC.

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 auprès d'un appareil iDRAC. Un seul objet Privilège peut être ajouté à un objet Association.

1. Sélectionnez l'onglet **Objet Privilège**, puis 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 auprès d'un appareil iDRAC. Un seul objet Privilège peut être ajouté à un objet Association.

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 périphériques iDRAC ou de groupes de périphériques iDRAC

Pour ajouter des périphériques iDRAC ou des groupes de périphériques iDRAC :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Entrez le nom des périphériques iDRAC ou des groupes de périphériques iDRAC, puis cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.
4. Cliquez sur l'onglet **Produits** pour ajouter un appareil iDRAC connecté au réseau, qui est disponible pour les utilisateurs et les groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs appareils iDRAC à un objet Association.

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. Utilisez les commandes suivantes :

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ActiveDirectory.RacName <RAC common name>
racadm set iDRAC.ActiveDirectory.RacDomain <fully qualified rac domain name>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
```

- Entrez le nom de domaine complet qualifié (FQDN) du contrôleur de domaine et non celui du domaine. Par exemple, saisissez `servername.dell.com` au lieu de `dell.com`.
- Vous devez fournir au moins une des trois adresses. L'iDRAC tente de se connecter à chacune des adresses configurées l'une après l'autre jusqu'à établir une connexion réussie. Avec le schéma étendu, il s'agit du nom de domaine qualifié ou des adresses IP des contrôleurs de domaine où se trouve le périphérique iDRAC.
- Pour désactiver la validation de certificat durant l'établissement d'une liaison SSL, utilisez la commande suivante :

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  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 l'établissement d'une liaison SSL (facultatif) :

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  Dans ce cas, vous devez téléverser un certificat d'autorité de certification en utilisant la commande suivante :

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

  REMARQUE : Si la validation de certificat est activée, spécifiez les adresses du serveur contrôleur de domaine et le FQDN. Assurez-vous que le DNS est correctement configuré sous **Paramètres iDRAC** > **Réseau**.

  L'utilisation de la commande RACADM suivante peut être facultative :

  ```
  racadm sslcertdownload -t 1 -f <RAC SSL certificate>
  ```

2. Si DHCP est activé sur l'iDRAC et que vous voulez utiliser le DNS fourni par le serveur DHCP, entrez la commande suivante :

   ```
   racadm set iDRAC.IPv4.DNSFromDHCP 1
   ```

3. Si le DHCP est désactivé sur l'iDRAC ou si vous voulez entrer manuellement votre adresse IP DNS, entrez la commande suivante :

   ```
   racadm set iDRAC.IPv4.DNSFromDHCP 0
   racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
   racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
   ```

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 iDRAC, entrez la commande suivante :

   ```
   racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
   domain controller>
   ```

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

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web iDRAC

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'iDRAC**.

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Services d'annuaire** > **Microsoft Active Directory**. Cliquez sur **Modifier**.
   La page **Configuration et gestion d'Active Directory - Étape 1 sur 4** s'affiche.
2. 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).
3. Cliquez sur **Next**.
   La page **Configuration et gestion d'Active Directory - Étape 2 sur 4** s'affiche.
4. Spécifiez les informations d'emplacement des serveurs Active Directory (AD) et des comptes d'utilisateur. Spécifiez également le délai pendant lequel l'iDRAC doit attendre les réponses d'AD lors du processus de connexion.

REMARQUE :

- Si la validation de certificat est activée, spécifiez les adresses du serveur contrôleur de domaine et le FQDN. Assurez-vous que le DNS est correctement configuré sous **Paramètres iDRAC** > **Réseau**.
- Si l'utilisateur et les objets iDRAC se trouvent dans des domaines différents, ne sélectionnez pas l'option **Domaine d'utilisateur depuis la connexion**. Sélectionnez plutôt l'option **Spécifier un domaine** et saisissez le nom de domaine dans lequel l'objet iDRAC est disponible.

5. Cliquez sur **Next**. La page **Configuration et gestion d'Active Directory -Étape 3 sur 4** s'affiche.
6. Sélectionnez **Schéma étendu** et cliquez sur **Suivant**.
   La page **Configuration et gestion d'Active Directory - Étape 4 sur 4** s'affiche.
7. Entrez le nom et l'emplacement de l'objet Périphérique iDRAC dans Active Directory (AD) et cliquez sur **Terminer**.
   Les paramètres Active Directory du mode Schéma étendu sont configurés.

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'iDRAC

Pour tester les paramètres Active Directory :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Services d'annuaire** > **Microsoft Active Directory**, puis cliquez sur **Tester**.
   La page **Test Active Directory Settings (Tester les paramètres Active Directory)** s'affiche.
2. Cliquez sur **Test**.
3. Entrez un nom d'utilisateur de test (par exemple, **utilisateur@domaine.com**) et le mot de passe, puis cliquez sur **Start Test (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, iDRAC impose que le serveur Active Directory soit identifié par le nom de domaine complet (FQDN) et non par une adresse IP. S'il est identifié par une adresse IP, la validation de certificat échoue, car l'iDRAC ne peut pas communiquer avec le serveur Active Directory.

Configuration d'utilisateurs LDAP générique

L'iDRAC fournit une solution générique de prise en charge de l'authentification basée sur le protocole LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne nécessite aucune extension de schéma sur vos services d'annuaire.

Pour rendre l'implémentation LDAP de l'iDRAC générique, les points communs entre les différents services d'annuaire sont utilisés pour regrouper les utilisateurs, puis mapper la relation utilisateur-groupe. L'action spécifique au service d'annuaire est le schéma. Par exemple, des noms d'attribut différents peuvent être attribués au groupe, à l'utilisateur et au lien entre l'utilisateur et le groupe. Ces actions peuvent être configurées dans l'iDRAC.

REMARQUE : StartTLS sur le port 389 est pris en charge. Par défaut, LDAPS sur le port 636 est configuré. Le protocole de connexion peut être reconfiguré sur StartTLS à l'aide de Redfish ou de la commande RACADM `racadm set iDRAC.LDAP.Connection StartTLS`.

REMARQUE : Les connexions Authentification à deux facteurs (TFA) par carte à puce et Authentification unique (SSO) ne sont pas prises en charge pour le service d'annuaire LDAP générique.

Configuration du service d'annuaire LDAP générique à l'aide de RACADM

Pour configurer le service d'annuaire LDAP, utilisez les objets des groupes `iDRAC.LDAP` et `iDRAC.LDAPRole`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web d'iDRAC

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'iDRAC**.

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Services de répertoire** > **Service de répertoire LDAP générique** et cliquez sur **Modifier**.
   La page **Configuration et gestion LDAP génériques - Étape 1 sur 3** affiche les paramètres LDAP génériques actuels.
2. Si vous le désirez, vous pouvez activer la validation de certificat et téléverser le certificat numérique utilisé au cours de l'initialisation des connexions SSL lors de la communication avec un serveur LDAP générique.
3. Cliquez sur **Next**.
   La page **Configuration et gestion LDAP génériques - Étape 2/3** s'affiche.
4. 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, spécifiez le nom de domaine complet qualifié du serveur LDAP et vérifiez que le DNS est correctement configuré sous **Paramètres iDRAC** > **Réseau**.

   REMARQUE : Dans cette version, le groupe imbriqué n'est pas pris en charge. Le firmware recherche le membre direct du groupe pour établir une correspondance avec le nom unique de l'utilisateur. En outre, un seul domaine est pris en charge. La gestion interdomaine n'est pas prise en charge.

5. Cliquez sur **Next**.
   La page **Configuration et gestion LDAP générique - Étape 3a/3** s'affiche.
6. Cliquez sur **Groupe de rôles**.
   La page **Configuration et gestion LDAP générique - Étape 3a/3** s'affiche.
7. 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 génériques - Étape 3a sur 3** affiche les paramètres de groupe de rôles.
8. Si vous voulez configurer d'autres groupes de rôles, répétez les étapes 7 et 8.
9. Cliquez sur **Terminer**. Le service d'annuaire LDAP générique est configuré.

Test des paramètres 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 à l'aide de l'interface Web d'iDRAC

Pour tester les paramètres du service d'annuaire LDAP :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **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 **Test**.
3. Saisissez le nom d'utilisateur et le mot de passe d'un utilisateur de répertoire choisi pour tester les paramètres LDAP. Le format dépend de l' **attribut de connexion** utilisé et le nom d'utilisateur saisi doit correspondre à la valeur de l'attribut choisi.

REMARQUE : Lorsque vous testez les paramètres LDAP avec **Enable Certificate Validation (Validation de certificat activée)**, iDRAC impose que le serveur LDAP soit identifié par le nom de domaine complet (FQDN) et non par une adresse IP. S'il est identifié par une adresse IP, la validation de certificat échoue, car l'iDRAC ne peut pas communiquer avec le serveur LDAP.

REMARQUE : Lorsque LDAP générique est activé, iDRAC tente d'abord de connecter l'utilisateur comme utilisateur de répertoire. S'il échoue, la recherche d'utilisateur local est activée.

Les résultats du test et le journal du test s'affichent.

12

Mode de verrouillage de la configuration du système

Le mode de verrouillage de la configuration du système permet d'éviter les modifications accidentelles après la configuration d'un système. Le mode de verrouillage s'applique à la fois aux mises à jour du firmware et à la configuration. Lorsque le système est verrouillé, toute tentative visant à modifier la configuration du système est bloquée. Si des tentatives sont effectuées pour modifier les paramètres système stratégiques, un message d'erreur s'affiche. L'activation du mode de verrouillage du système bloque la mise à jour du firmware des cartes d'E/S tierces à l'aide des outils fournisseurs.

Le mode System Lockdown est disponible uniquement pour les clients disposant d'une licence Grand compte.

REMARQUE : Le verrouillage optimisé pour les cartes NIC inclut uniquement le verrouillage du firmware pour empêcher les mises à jour de ce dernier. Le verrouillage de la configuration (x-UEFI) n'est pas pris en charge.

REMARQUE : Une fois le mode System Lockdown activé, vous ne pouvez plus modifier les paramètres de configuration. Les champs Paramètres système sont désactivés.

Le mode de verrouillage peut être activé ou désactivé en utilisant les interfaces suivantes :

- Interface web iDRAC
- RACADM
- Profil de configuration système (SCP)
- Redfish
- Utilisation de F2 durant le POST et sélection des paramètres iDRAC
- Effacement du système d'usine

REMARQUE : Pour activer le mode Verrouillage, vous devez disposer d'une licence iDRAC Enterprise ou Datacenter et de privilèges système de contrôle et de configuration.

REMARQUE : Vous pouvez accéder à vMedia alors que le système est en mode Verrouillage mais la configuration du partage de fichier à distance n'est pas activée.

REMARQUE : Les interfaces telles que OMSA, SysCfg et USC peuvent uniquement vérifier les paramètres, mais ne peuvent pas modifier les configurations.

REMARQUE : Une fois le mode Verrouillage activé, vous ne pouvez pas configurer les paramètres d'alerte. Vous pouvez toutefois déclencher un e-mail de test.

Le tableau suivant répertorie les fonctionnalités actives et inactives, les interfaces et utilitaires qui sont affectés par le mode Verrouillage :

REMARQUE : La modification de l'ordre de démarrage avec le contrôleur iDRAC n'est pas prise en charge lorsque le mode Verrouillage est activé. Cependant, l'option de contrôle au démarrage est disponible dans le menu de vConsole, et n'a aucun effet lorsque l'iDRAC est en mode Verrouillage.

Tableau 33. Éléments affectés par le mode de verrouillage

Désactivé	Toujours actifs
• Suppression de licences • Mises à jour du DUP • Importation SCP • Restauration des valeurs par défaut • IPMI • DRAC/LC • DTK-Syscfg • Redfish • OpenManage Essentials • BIOS (paramètres F2 en lecture seule)	• Opérations d'alimentation : mise sous tension/hors tension, réinitialisation • Paramètre du seuil énergétique • Priorité d'alimentation • Identification des appareils (châssis ou contrôleur PERC) • Remplacement de pièces, restauration facile et remplacement de la carte système • Exécution de tests de diagnostic • Opérations modulaires (FlexAddress ou adresse attribuée à distance)

Tableau 33. Éléments affectés par le mode de verrouillage

Désactivé	Toujours actifs

• Sélection de cartes réseau
• iLKM/SEKM
	• Tous les outils fournisseurs ayant un accès direct à l'appareil (à l'exception des cartes NIC sélectionnées)
	• Exportation de licence
	• PERC
	  ○ PERC CLI
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• Tous les outils fournisseurs ayant un accès direct à l'appareil
	• NVMe
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• BOSS-N1
	• Paramètres ISM (activation BMC du système d'exploitation, ping du minuteur de surveillance, nom du système d'exploitation, version du système d'exploitation)

REMARQUE : Lorsque le mode de verrouillage est activé, l'option de connexion OpenID Connect ne s'affiche pas dans la page de connexion de l'iDRAC.

13

Configuration de l'iDRAC pour l'authentification unique ou par carte à puce

Cette section fournit des informations sur la configuration d'iDRAC pour la connexion à l'aide d'une carte à puce (pour les utilisateurs locaux et Active Directory) et pour l'authentification unique (SSO) (pour les utilisateurs Active Directory.) L'authentification unique et la connexion avec une carte à puce sont des fonctions disponibles sous licence.

iDRAC prend en charge l'authentification Active Directory basée sur Kerberos pour les connexions par carte à puce et SSO. Pour plus d'informations sur Kerberos, consultez le site Web de Microsoft.

Sujets :

Exigences d'ouverture de session Active Directory par connexion directe ou carte à puce

Les exigences de connexion directe ou de connexion avec une carte à puce sont les suivantes :

- Synchronisez l'heure de l'iDRAC sur l'heure du contrôleur de domaine Active Directory. Dans le cas contraire, l'authentification Kerberos sur l'iDRAC échoue. Vous pouvez utiliser la fonctionnalité Fuseau horaire et NTP pour synchroniser l'heure. Pour ce faire, reportez-vous à la section Configuration du fuseau horaire et du NTP.
- Enregistrez iDRAC comme un ordinateur dans le domaine racine Active Directory.

  REMARQUE : iDRAC ne prend pas en charge les utilisateurs de cartes à puce PIV (Personal Identity Verification) ou CAC (Common Access Card) sur un domaine enfant ou un sous-domaine dans une forêt ou un ensemble de domaines. Pour contourner cette restriction, il est recommandé de déployer tous les utilisateurs de cartes à puce sur le domaine racine et non sur les domaines enfants dans la forêt.

- 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 (Kerberos uniquement)** est sélectionnée dans l'onglet **Délégation** pour l'utilisateur keytab. Cet onglet est disponible uniquement après la création du fichier keytab à l'aide de 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 (SSO), configurez la zone de recherche inverse sur les serveurs DNS du sous-réseau où se trouve iDRAC.

  REMARQUE : Si le nom d'hôte ne correspond pas à la recherche DNS inverse, l'authentification Kerberos échoue.

- Configurez le navigateur pour prendre en charge la connexion SSO. Pour plus d'informations, consultez authentification unique.

  REMARQUE : Google Chrome et Safari ne prennent pas en charge Active Directory pour la connexion SSO.

Enregistrement iDRAC sur un système de nom de domaine

Pour enregistrer iDRAC dans un domaine racine Active Directory :

1. Cliquez sur **Paramètres iDRAC** > **Connectivité** > **Réseau**.
   La page **Réseau** s'affiche.
2. Vous pouvez sélectionner **Paramètres IPv4** ou **Paramètres IPv6** en fonction des paramètres IP.
3. Fournir une adresse IP valide de **Serveur DNS préféré/secondaire**. Cette valeur est une adresse IP valide de serveur DNS qui fait partie du domaine racine.
4. Sélectionnez **Enregistrer iDRAC auprès du DNS.**
5. Spécifiez un **nom de domaine DNS**.
6. 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'iDRAC**.

Création d'objets Active Directory et fourniture de privilèges

Connexion par authentification unique avec un schéma standard Active Directory

Procédez comme suit pour la connexion par authentification unique avec un schéma standard Active Directory :

1. Créez un groupe d'utilisateurs.
2. Créez un utilisateur pour le schéma standard.

REMARQUE : Utilisez le groupe d'utilisateurs AD et l'utilisateur AD existants.

Connexion par authentification unique avec un schéma étendu Active Directory

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 Privilèges créé.

   REMARQUE : 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. Accordez un privilège d'accès aux **utilisateurs authentifiés** afin de leur permettre d'accéder à l'objet Association créé.

Connexion par authentification unique à Active Directory

Procédez comme suit pour la connexion par authentification unique à Active Directory :

1. Créez un utilisateur Kerberos pour l'onglet clé qui est utilisé pour la création du fichier de l'onglet clé.

REMARQUE : Créez une nouvelle clé KERBEROS pour chaque adresse IP de l'iDRAC.

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

Avant de configurer l'ouverture de session par connexion directe iDRAC pour Active Directory, veillez à exécuter toutes les tâches préalables requises.

Vous pouvez configurer iDRAC pour une connexion directe Active Directory lorsque vous définissez un compte d'utilisateur basé sur Active Directory.

Création d'un utilisateur dans Active Directory avec authentification unique

Pour créer un utilisateur dans Active Directory avec authentification unique :

1. Créez un nouvel utilisateur dans l'unité d'organisation.
2. Rendez-vous sur **Utilisateur Kerberos>Propriétés>Compte>Utiliser les types de chiffrement AES pour ce compte**
3. Utilisez la commande suivante pour générer un fichier keytab Kerberos dans le serveur Active Directory :

```
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
```

Remarque pour le schéma étendu

- Modifiez le paramètre Délégation de l'utilisateur Kerberos.
- Rendez-vous sur **Utilisateur Kerberos >Propriétés>Délégation>Faire confiance à cet utilisateur pour la délégation à n'importe quel service (Kerberos uniquement)**

REMARQUE : Déconnectez-vous et connectez-vous à l'aide de l'utilisateur Active Directory de la station de gestion après la modification du paramètre ci-dessus.

Génération d'un fichier Keytab Kerberos

Pour prendre en charge l'authentification d'ouverture de session par connexion directe (SSO) ou par carte à puce, iDRAC prend en charge la configuration pour s'activer comme service Kerberos sur un réseau Kerberos Windows. La configuration Kerberos sur l'iDRAC implique les mêmes étapes que la configuration d'un service Kerberos de serveur autre que Windows en tant qu'entité de sécurité principale dans Windows Server Active Directory.

L'outil **ktpass** (disponible dans Microsoft avec le CD/DVD d'installation du serveur) est utilisé pour créer des liaisons SPN (Service Principal Name) avec un compte d'utilisateur et exporter les informations de confiance dans un fichier **keytab** Kerberos de style MIT, ce qui permet 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 de chiffrement utilisée pour chiffrer les informations entre le serveur et le KDC. L'outil ktpass permet aux services basés sur UNIX qui prennent en charge l'authentification Kerberos d'utiliser les fonctionnalités d'interopérabilité fournies par service KDC d'un serveur Windows Kerberos. Pour plus d'informations sur l'utilitaire **ktpass**, voir le site Web de 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 du DNS iDRAC vers lequel vous téléchargez 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 adresser iDRAC à un compte d'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 chiffrement est AES256-SHA1. Le type principal est KRB5_NT_PRINCIPAL. La propriété **Utiliser les types de chiffrement AES 256 pour ce compte** doit être activée dans les propriétés du compte d'utilisateur auquel le nom SPN est adressé.

REMARQUE : Utilisez des minuscules pour **iDRACname** et **Service Principal Name**. Utilisez des majuscules pour le nom de domaine, comme indiqué dans l'exemple.

Un fichier keytab est généré.

REMARQUE : Si vous rencontrez des problèmes avec l'utilisateur iDRAC pour lequel le fichier keytab est créé, créez un utilisateur et un nouveau fichier keytab. Si le fichier keytab initialement créé est à nouveau exécuté, il n'est pas configuré correctement.

Configuration d'ouverture de session dans l'iDRAC par connexion directe (SSO) pour les utilisateurs Active Directory à l'aide de l'interface Web

Pour configurer l'ouverture de session dans iDRAC par connexion directe (SSO) pour Active Directory :

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

1. Vérifiez si le nom DNS de l'iDRAC correspond au nom de domaine complet qualifié de l'iDRAC. Pour ce faire, dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Réseau** > **Paramètres communs** et reportez-vous à la propriété **Nom iDRAC 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 iDRAC par connexion directe (SSO) pour les utilisateurs Active Directory à l'aide de RACADM

Pour activer l'ouverture de session directe SSO, configurez Active Directory et exécutez la commande suivante :

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

Paramètres de la station de gestion

Effectuez les opérations suivantes après la configuration de la connexion par authentification unique pour les utilisateurs Active Directory :

1. Définissez l'adresse IP du serveur DNS dans les propriétés du réseau et mentionnez l'adresse IP préférée du serveur DNS.
2. Accédez à Ordinateur et ajoutez le domaine ***domain.tld**.
3. Ajoutez l'utilisateur Active Directory à Administrateur en naviguant jusqu'à : **Ordinateur** > **Gérer** > **Utilisateur local et groupes** > **Groupes** > **Administrateur** et ajoutez l'utilisateur Active Directory.
4. Déconnectez le système et connectez-vous à l'aide des informations d'identification de l'utilisateur Active Directory.
5. Dans Paramètres d'Internet Explorer, ajoutez le domaine *domain.tld comme suit :
   a. Accédez à **Outils** > **Options Internet** > **Sécurité** > **Internet local** > **Sites** et désactivez **Détecter automatiquement le paramètre de réseau intranet**. Sélectionnez les trois autres options, puis cliquez sur **Avancé** pour ajouter *domain.tld
   b. Ouvrez une nouvelle fenêtre dans Internet Explorer et utilisez le nom d'hôte de l'iDRAC pour lancer l'interface utilisateur graphique de l'iDRAC.
6. Dans les paramètres de Mozilla Firefox, ajoutez le domaine *domain.tld :
   - Lancez le navigateur Firefox et saisissez about:config dans l'URL.
   - Utilisez le filtre Négociation dans la zone de texte. Double-cliquez sur le résultat composé d'**auth.trusted.uris**. Saisissez le domaine, enregistrez les paramètres et fermez le navigateur.
   - Ouvrez une nouvelle fenêtre dans Firefox et utilisez le nom d'hôte de l'iDRAC pour lancer l'interface utilisateur graphique de l'iDRAC.

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

Avant d'activer ou désactiver l'ouverture de session par carte à puce pour iDRAC, vérifiez que :

- Vous disposez des autorisations de configuration iDRAC.
- La configuration d'utilisateur local iDRAC ou Active Directory avec les certificats appropriés est terminée.

REMARQUE : Si la connexion par carte à puce est activée, les options SSH, IPMI sur le LAN, Série sur LAN et Interface RACADM à distance sont désactivées. Encore une fois, si vous désactivez la connexion par carte à puce, les interfaces ne sont pas activées automatiquement.

Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de l'interface Web

Pour activer ou désactiver la fonction d'ouverture de session par carte à puce :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Carte à puce**.
   La page **Carte à puce** s'affiche.
2. Dans le menu déroulant **Configurer l'ouverture de session par carte à puce**, sélectionnez **Activé** pour activer l'ouverture de session par carte à puce ou sélectionnez **Activé avec l'interface RACADM distante**. Autrement, sélectionnez **Désactivé**.

   Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.
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'iDRAC.

Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de l'interface RACADM

Pour activer la connexion par carte à puce, utilisez la commande `set` avec des objets du groupe `iDRAC.SmartCard`.

Pour en savoir plus, voir le *Guide de la CLI RACADM de l'iDRAC (Integrated Dell Remote Access Controller)*.

Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de 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 l'ouverture de session par carte à puce. Autrement, sélectionnez **Désactivé**. Pour plus d'informations sur ces options, voir l'**Aide en ligne de l'utilitaire de configuration de l'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.

Configuration de la connexion par carte à puce

REMARQUE : Pour la configuration de la carte à puce Active Directory, l'iDRAC doit être configuré pour une connexion par authentification unique avec un schéma standard ou étendu.

Configuration de la connexion par carte à puce iDRAC pour les utilisateurs Active Directory

Avant de configurer l'ouverture de session dans iDRAC par carte à puce pour les utilisateurs Active Directory, veillez à exécuter préalablement les tâches requises.

Pour configurer l'ouverture de session iDRAC par carte à puce :

1. Dans l'interface Web iDRAC, lors de la configuration d'Active Directory pour définir un compte d'utilisateur basé sur le schéma standard ou étendu, dans la page **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'iDRAC**.

Configuration d'ouverture de session iDRAC par carte à puce pour les utilisateurs locaux

Pour configurer un utilisateur local iDRAC pour la connexion par carte à puce :

1. Téléchargez le certificat d'utilisateur de carte à puce et le certificat CA autorisé vers l'iDRAC.
2. Activez l'ouverture de session par carte à puce

Téléversement du certificat d'utilisateur de carte à puce

Avant de charger le certificat d'utilisateur, veillez à exporter le certificat du fournisseur de la carte à puce au format Base64. Les certificats SHA-2 sont également pris en charge.

Téléversement d'un certificat d'utilisateur de carte à puce à l'aide de l'interface Web

Pour téléverser un certificat d'utilisateur de carte à puce :

1. Dans l'interface Web de l'iDRAC, accédez à **Paramètres iDRAC** > **Utilisateurs** > **Carte à puce**.

   REMARQUE : La fonctionnalité de connexion par carte à puce nécessite la configuration du certificat utilisateur local et/ou Active Directory.

2. Sous **Configurer la connexion par carte à puce**, sélectionnez **Activer avec RACADM à distance** pour activer la configuration.
3. Réglez l'option sur **Activer le contrôle CRL pour la connexion par carte à puce**.
4. Cliquez sur **Appliquer**.

Téléversement d'un certificat d'utilisateur de carte à puce en à l'aide de RACADM

Pour télécharger un certificat d'utilisateur de carte à puce, utilisez l'objet **usercertupload**. Pour plus d'informations, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Demande de certificat d'inscription de la carte à puce

Procédez comme suit pour demander le certificat d'inscription de la carte à puce :

1. Connectez la carte à puce dans le système client et installez les pilotes et logiciels nécessaires.
2. Vérifiez l'état du pilote dans le Gestionnaire de périphériques.
3. Lancez l'agent d'inscription de la carte à puce dans le navigateur.
4. Saisissez le **Nom d'utilisateur** et le **Mot de passe** et cliquez sur **OK**.
5. Cliquez sur **Demande de certificat**.
6. Cliquez sur **Demande de certificat avancée**.
7. Cliquez sur **Demander un certificat** pour une carte à puce au nom d'un autre utilisateur en utilisant la station d'inscription de certificat de la carte à puce.
8. Sélectionnez l'utilisateur à inscrire en cliquant sur le bouton **Sélectionner un utilisateur**.
9. Cliquez sur **Inscrire** et saisissez les informations d'identification de la carte à puce.
10. Saisissez le code PIN de la carte à puce, puis cliquez sur **Envoyer**.

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.

Téléversement d'un certificat d'autorité de certification de confiance pour une carte à puce à l'aide de 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 de l'iDRAC, accédez à **Paramètres iDRAC** > **Réseau** > **Authentification utilisateur** > **Utilisateurs locaux**. La page **Utilisateurs** s'affiche.

2. Dans la colonne **ID utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configurations de cartes à puce**, 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 à l'aide de 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 en savoir plus, voir le *Guide de la CLI RACADM de l'iDRAC (Integrated Dell Remote Access Controller)*.

Connexion à l'aide de la carte à puce

REMARQUE : La connexion par carte à puce est prise en charge dans Edge/Chrome et FireFox.

REMARQUE : La connexion par carte à puce est prise en charge uniquement avec la version TLS 1.2.

Pour vous connecter à l'aide d'une carte à puce :

1. Déconnectez-vous de l'interface utilisateur graphique de l'iDRAC après l'activation de la carte à puce.
2. Lancez l'iDRAC via `http://IP/` ou à l'aide du FQDN `http://FQDN/`
3. Cliquez sur **Installer** une fois le plug-in de la carte à puce téléchargé.
4. Saisissez le code PIN de la carte à puce, puis cliquez sur **Envoyer**.
5. L'IDRAC se connecte avec succès à l'aide de la carte à puce.

14

Configuration d'iDRAC 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 système est supérieur à la condition prédéfinie. Si un évènement correspond à un filtre d'évènement et que vous avez configuré ce filtre afin de générer une alerte (E-mail, interruption SNMP, Alerte IPMI, Journaux système distant, Évènements Redfish ou Évènements WS), l'alerte est envoyée à une ou plusieurs destinations configurées. Si ce même filtre d'événement est également configuré pour effectuer une action (comme un redémarrage, un cycle d'alimentation ou une mise hors tension du système), l'action est effectuée. Vous ne pouvez configurer qu'une seule action pour chaque événement.

Pour configurer iDRAC 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, les événements Redfish, 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, des événements Redfish, 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.

REMARQUE : Pour toute mise à jour nécessitant une réinitialisation/redémarrage de l'iDRAC ou si l'iDRAC est redémarré, il est recommandé de vérifier si l'iDRAC est prêt en attendant quelques secondes, avec un délai d'expiration maximum de 5 minutes, avant d'utiliser une autre commande.

Sujets :

Activation ou désactivation des alertes

Pour envoyer une alerte à des destinations configurées ou pour exécuter une action d'événement, vous devez activer l'option d'envoi d'alertes globales. Cette propriété remplace les actions d'envoi d'alertes ou d'événement individuelles définies.

Activation ou désactivation des alertes à l'aide de l'interface Web

Pour activer ou désactiver la génération d'alertes :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Configuration d'alerte**.
   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.

Configuration d'une alerte rapide

Pour configurer les alertes en masse :

1. Accédez à **Configuration d'alerte rapide** sous la page **Configuration d'alerte**.
2. Sous la section **Configuration d'alerte rapide** :
   - Sélectionnez la catégorie d'alerte.
   - Sélectionnez la notification de gravité du problème.
   - Sélectionnez l'emplacement où vous souhaitez recevoir ces notifications.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.
   Toutes les alertes configurées s'affichent sous **Récapitulatif de la configuration des alertes**.

REMARQUE : Vous devez sélectionner au moins une catégorie, une gravité et un type de destination à appliquer à la configuration.

REMARQUE : Après avoir configuré les alertes à l'aide de l'onglet **Alertes rapides**, lorsque vous passez à l'onglet **Configuration d'alerte**, les alertes configurées ne sont pas activées dans les catégories d'alertes respectives. Pour activer les catégories d'alertes respectives :

1. Sélectionnez l'un des autres onglets de catégorie (**État de santé du système**, **Audit**, **Mises à jour** et **Configuration**) dans la page **Configuration d'alerte**.
2. Revenez à la catégorie utilisée initialement pour la configuration d'alerte.

Activation ou désactivation des alertes à l'aide de RACADM

Utilisez la commande suivante :

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 — Désactivé

n=1 — Activé

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 de l'iDRAC** s'affiche.
2. Sous **Événements de plateforme**, sélectionnez **Activé** pour activer la génération d'alertes ou l'action d'événement. Autrement, sélectionnez **Désactivé**. Pour plus d'informations sur ces options, voir l'**Aide en ligne de l'utilitaire de configuration de l'iDRAC**.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres d'alerte sont définis.

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.

Définition d'alertes d'événements à l'aide de l'interface Web

Pour définir une alerte d'événement à l'aide de 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. Dans l'interface Web iDRAC, accédez à **Configuration** > **Paramètres système** > **Configuration des alertes et du journal système distant**.
3. Sous **Catégorie**, sélectionnez une alerte ou toutes les alertes suivantes des événements requis :
   - E-mail
   - Interruption SNMP
   - Alerte IPMI
   - Journal système distant
   - Événements WS
   - Journal du SE
   - Événement Redfish
4. Sélectionnez **Action**.
   Le paramétrage est enregistré.
5. Vous pouvez également envoyer un événement test. Dans le champ **ID de message d'événement ID**, entrez l'ID du message à tester si l'alerte est générée, puis cliquez sur **Tester**. Pour plus d'informations sur les messages d'événements et d'erreurs générés par le firmware du système et les agents qui surveillent les composants du système, voir le **Guide de référence Dell des messages d'événement et d'erreur** sur iDRACmanuals.

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, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Définition d'événement de récurrence d'alerte

Vous pouvez configurer l'iDRAC pour générer des événements supplémentaires à des intervalles spécifiques, si le système continue de fonctionner à une température 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 366 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 RACADM

Pour définir l'événement de récurrence d'alerte à l'aide de RACADM, utilisez la commande **eventfilters**. Pour plus d'informations, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Définition d'événements de récurrence d'alerte à l'aide de l'interface Web iDRAC

Pour définir la valeur de récurrence d'alerte :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Récurrence des alertes**.
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 de l'iDRAC**.
3. Cliquez sur **Appliquer**.
   Les paramètres de récurrence d'alerte sont enregistrés.

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.

Définition d'actions d'événement à l'aide de l'interface Web

Pour configurer une action :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Configuration des alertes et du journal système distant**.
2. Dans le menu déroulant **Actions** de chaque événement, sélectionnez une action :
   - Redémarrage
   - Cycle d'alimentation
   - Mettre hors tension
   - Pas d'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 la commande `eventfilters`. Pour plus d'informations, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI

La station de gestion utilise des interruptions SNMP (Simple Network Management Protocol) et IPMI (Intelligent Platform Management Interface) pour recevoir les données de l'iDRAC. Pour les systèmes dotés d'un grand nombre de nœuds, il peut s'avérer inefficace pour une station de gestion d'interroger chaque contrôleur iDRAC pour chaque condition susceptible de se produire. Par exemple, les interruptions d'événements peuvent aider une station de gestion à équilibrer la charge entre les nœuds ou à émettre une alerte en cas d'échec de l'authentification. Les formats SNMP v1, v2 et v3 sont pris en charge.

Vous pouvez configurer les destinations d'alerte IPv4 et IPv6, les paramètres e-mail et les paramètres de serveur SMTP et tester ces paramètres. Vous pouvez par ailleurs spécifier l'utilisateur SNMP v3 auquel vous souhaitez envoyer les interruptions SNMP.

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.

Configuration des destinations d'alerte IP

Vous pouvez configurer des adresses IPv6 ou IPv4 pour recevoir les alertes IPMI ou les interruptions SNMP.

Pour en savoir plus sur les MIB iDRAC requises pour surveiller les serveurs à l'aide de SNMP, voir *Guide de référence SNMP Dell OpenManage* disponible sur la page des manuels OpenManage..

Configuration de destinations d'alerte IP à l'aide de l'interface Web

Pour configurer les paramètres des destinations d'alerte à l'aide de l'interface Web :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres SNMP et de messagerie**.
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 plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.
3. Sélectionnez l'utilisateur SNMP v3 auquel vous voulez envoyer l'interruption SNMP.
4. Entrez la chaîne de communauté SNMP iDRAC (applicable uniquement pour SNMPv1 et v2) et le numéro de port de l'alerte SNMP.
   Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

REMARQUE : La valeur Chaîne de communauté indique la chaîne de communauté à utiliser dans une interruption d'alerte SNMP (Simple Network Management Protocol) envoyée depuis l'iDRAC. Assurez-vous que la chaîne de communauté de destination est identique à la chaîne de communauté de l'iDRAC. La valeur par défaut est Publique.

5. 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.
6. Cliquez sur **Appliquer**.
   Les destinations d'alerte sont configurées.
7. 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**, **SNMP v2** ou **SNMP v3**) 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 à l'aide de RACADM

Pour définir les paramètres d'alerte d'interruption :

1. Pour activer les interruptions :

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

Paramètre	Description
<index>	Index de destination. Les valeurs autorisées sont comprises entre 1 et 8.
<n>=0 **<n>**=1	Désactiver l'interruption Activer l'interruption

2. Pour définir l'adresse de destination d'interruption :

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

Paramètre	Description
<index>	Index de destination. Les valeurs autorisées sont comprises entre 1 et 8.
<Address>	Une adresse IPv4, IPv6 ou FQDN valide

3. Configurez la chaîne de nom de communauté SNMP :

```
racadm set idrac.ipmilan.communityname <community_name>
```

Paramètre	Description
<community_name>	Le nom de communauté SNMP.

4. Pour configurer la destination SNMP :
   - Définir la destination d'interruptions SNMP pour SNMPv3 :

     ```
     racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
     ```

   - Définir les utilisateurs SNMPv3 pour les destinations des interruptions :

     ```
     racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
     ```

- Activer SNMPv3 pour un utilisateur :

  ```
  racadm set idrac.users.<index>.SNMPv3Enable Enabled
  ```

5. Pour tester l'interruption, si nécessaire :

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

Pour plus d'informations, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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 de configuration de l'iDRAC. Pour ce faire :

1. Dans l'**utilitaire de configuration d'iDRAC**, accédez à **Alertes**.
   La page **Paramètres d'alerte de l'iDRAC** s'affiche.
2. Sous **Paramètres d'interruption**, activez la ou les adresses IP pour recevoir les interruptions et saisissez la ou les adresses IPv4, IPv6 ou FQDN de destination. Vous pouvez spécifier 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 de l'expéditeur et l'adresse e-mail du destinataire (destination) pour recevoir les alertes par e-mail. Configurez également les paramètres de l'adresse du serveur SMTP.

REMARQUE : Les alertes e-mail prennent en charge les adresses IPv4 et IPv6. Le nom de domaine DNS de l'iDRAC doit être spécifié lors de l'utilisation d'adresses IPv6.

REMARQUE : Si vous utilisez un serveur SMTP externe, assurez-vous que l'iDRAC puisse communiquer avec lui. Si le serveur est inaccessible, le message d'erreur RAC0225 s'affiche lors de la tentative d'envoi d'un e-mail de test.

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. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Configuration SMTP (e-mail)**.
2. Saisissez une adresse e-mail valide.
3. Cliquez sur **Envoyer** sous **E-mail test** pour tester les paramètres des alertes par e-mail.
4. Cliquez sur **Appliquer**.
5. Pour les paramètres du serveur SMTP (E-mail), fournissez les informations suivantes :
   - Adresse IP du serveur SMTP (e-mail) ou nom FQDN/DNS
   - Adresse expéditeur personnalisée : ce champ contient les options suivantes :
     - **Par défaut** : le champ Adresse n'est pas modifiable.
     - **Personnalisé** : vous pouvez saisir l'ID d'e-mail à partir duquel vous pouvez recevoir les alertes par e-mail.
   - Préfixe d'objet de message personnalisé : ce champ contient les options suivantes :
     - **Par défaut** : le message par défaut n'est pas modifiable.
     - **Personnalisé** : vous pouvez choisir le message à afficher dans la ligne **Objet** de l'e-mail.
   - Numéro de port SMTP : la connexion peut être chiffrée et des e-mails peuvent être envoyés via des ports sécurisés :
     - **Pas de chiffrement** : port 25 (valeur par défaut)
     - **SSL** : port 465
   - Chiffrement de la connexion : lorsque vous ne disposez pas d'un serveur de messagerie sur votre site, vous pouvez utiliser des serveurs de messagerie basés dans le Cloud ou sur des relais SMTP. Pour configurer le serveur de messagerie dans le Cloud, vous pouvez sélectionner l'une des valeurs suivantes pour cette fonctionnalité dans la liste déroulante :

- **Aucun** : aucun chiffrement sur la connexion au serveur SMTP. Il s'agit de la valeur par défaut.
- **SSL** : exécute le protocole SMTP sur SSL.

REMARQUE :
- Il s'agit d'une fonctionnalité sous licence, qui n'est pas disponible avec la licence iDRAC Core
- Vous devez disposer du privilège Configurer l'iDRAC pour pouvoir utiliser cette fonctionnalité.

- Authentification
- Nom d'utilisateur

Pour les paramètres du serveur, l'utilisation du port dépend du paramètre `connectionencryptiontype` et il ne peut être configuré qu'à l'aide de RACADM.

6. Cliquez sur **Appliquer**. Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

Définition des paramètres des alertes par e-mail à l'aide de RACADM

1. Pour activer les alertes par e-mail :

```
racadm set iDRAC.EmailAlert.Enable.[index] [n]
```

Paramètre	Description
index	Index de destination d'e-mail. Les valeurs autorisées sont comprises entre 1 et 4.
n=0	Désactive les alertes par e-mail.
n=1	Active les alertes par e-mail.

2. Pour configurer les paramètres de l'e-mail :

```
racadm set iDRAC.EmailAlert.Address.[index] [email-address]
```

Paramètre	Description
index	Index de destination d'e-mail. Les valeurs autorisées sont comprises entre 1 et 4.
email-address	Adresse e-mail de destination qui reçoit les alertes d'événements de la plate-forme.

3. Pour configurer les paramètres de l'e-mail de l'expéditeur :

```
racadm set iDRAC.RemoteHosts.[index] [email-address]
```

Paramètre	Description
index	Index de l'e-mail de l'expéditeur.
email-address	Adresse e-mail de l'expéditeur des alertes d'événements de la plate-forme.

4. Pour configurer un message personnalisé :

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

Paramètre	Description
index	Index de destination d'e-mail. Les valeurs autorisées sont comprises entre 1 et 4.
custom-message	Message personnalisé

5. Pour tester l'alerte par e-mail configurée, si nécessaire :

```
racadm testemail -i [index]
```

Paramètre	Description
index	Index de destination de l'e-mail à tester. Les valeurs autorisées sont comprises entre 1 et 4.

Pour plus d'informations, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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 serveur de messagerie SMTP à l'aide de l'interface Web de l'iDRAC

Pour définir l'adresse du serveur SMTP :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Configuration des alertes** > **Configuration SMTP (e-mail)**.
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 de l'iDRAC**.
5. Cliquez sur **Appliquer**.
   Les paramètres SMTP sont définis.

Définition des paramètres d'adresse du serveur de messagerie SMTP à l'aide de RACADM

Pour configurer les paramètres SMTP de serveur de messagerie :

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

Configuration des événements Redfish

Le protocole d'événements Redfish permet à un service client (abonné) de manifester un intérêt (abonnement) auprès d'un serveur (source d'événement) en vue de recevoir des messages contenant les événements Redfish (notifications ou messages d'événement). Les clients qui souhaitent recevoir les messages d'événements Redfish peuvent s'abonner à l'iDRAC afin de recevoir les événements liés aux tâches Lifecycle Controller.

Configuration de la journalisation d'un système distant

Vous pouvez envoyer des journaux lifecycle à un système distant. Avant, assurez-vous que :

- Il existe une connectivité réseau entre l'iDRAC et le système distant.
- Le système distant et l'iDRAC se trouvent dans le même réseau.

REMARQUE : Cette fonctionnalité est disponible avec les licences iDRAC Enterprise et Datacenter.

Un certificat d'identité de serveur Syslog distant peut être généré dans la configuration du serveur de signature de certificat interne de la société. Les serveurs et clients Syslog distants basés sur TLS utilisent le même certificat d'autorité de certification dans les paramètres de configuration, qui est obtenu à partir d'un serveur d'autorité de certification. L'iDRAC fournit l'interface utilisateur qui permet de télécharger ce certificat d'autorité de certification, de l'ajouter à son fichier de configuration et de redémarrer le service Sylog distant.

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 de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Configuration des alertes** > **Syslog distant** > **Paramètres**.
2. Les options suivantes sont disponibles. Sélectionnez les propriétés requises :
   - **Paramètres de base** – pour les solutions existantes
   - **Paramètres sécurisés** – pour la nouvelle implémentation (chiffrer le trafic Syslog distant avec TLS). Pour
   - **Aucun** – pour désactiver les alertes Syslog distantes

   Pour plus d'informations sur les champs, voir l'**aide en ligne de l'iDRAC**.
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 à l'aide de RACADM

Pour configurer les paramètres de consignation d'un système distant, utilisez la commande `set` avec les objets du groupe `iDRAC.SysLog`.

Pour plus d'informations, consultez le document Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

ID de message d'alerte

Le tableau suivant répertorie les ID de message affichés pour les alertes.

Tableau 34. ID de message d'alerte

ID du message	Description
AMP	Ampérage
ASR	Réinitialisation automatique du système
BAT	Événement de batterie
BIOS	Gestion du BIOS
AMORÇAGE	Contrôle de l'amorçage
CBL	Câble
Processeur	Processeur
CPUA	Proc absent
CTL	Contrôle stockage
DH	Gestion cert
DIS	Détection automatique
ENC	Boîtier de stockage
VENTILATEUR	Événement ventilateur
FSD	Débogage
HWC	Configuration matérielle
IPA	Changement d'adresse IP DRAC
ITR	Intrusion

Tableau 34. ID de message d'alerte (suite)

ID du message	Description
JCP	Contrôle des tâches
LC	Lifecycle Controller
LIC	Licences
LNK	Condition de la liaison
LOG	Consigner un événement
MÉM	Mémoire
NDR	Pilote SE NIC
Carte NIC	Configuration NIC
OSD	Déploiement du SE
OSE	Événement OS
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
ROUGE	Téléchargement FW
RFM	SD FlexAddress
RSI	Service à distance
SEC	Événement sécurité
Journal d'évènements système	Journal des événements système
SRD	RAID logiciel
Disque SSD	SSD PCIe
STOR	Stockage
SUP	Tâche de mise à jour FW
SWC	Configuration logicielle
SWU	Changement logiciel
SYS	System Info (Informations sur le système)
TMP	Température
TST	Alerte test
UEFI	Événement UEFI
USR	Suivi utilisateur
VDR	Disque virtuel
VLT	Tension

Tableau 34. ID de message d'alerte (suite)

ID du message	Description
VME	Support virtuel
VRM	Console virtuelle
WRK	Note de travail

Détection de fuite au niveau du processeur et du processeur graphique

L'iDRAC détecte les fuites de liquide de refroidissement dans le processeur et le processeur graphique par le biais de signaux critiques, d'avertissement et d'information provenant des capteurs IPMI OEM correspondants. Les fuites sont notifiées sous forme de journaux d'événements système (SEL), de journaux LC, d'événements WS, d'e-mails et d'interruptions SNMP en fonction des paramètres d'alerte configurés. L'iDRAC effectue les actions appropriées en fonction des paramètres de configuration des alertes.

Par défaut, l'alerte **Système de refroidissement liquide Action par défaut Mise hors tension** entraîne une **mise hors tension normale** en cas de fuite du processeur graphique dans le serveur. Lorsque vous remarquez une fuite du processeur graphique, il est recommandé de forcer la mise hors tension du serveur et de ne pas attendre la fin de la **mise hors tension normale**.

Si l'iDRAC détecte une fuite du processeur graphique lors de l'accès à l'interface utilisateur LC ou à l'environnement de pré-démarrage (BIOS ou gestionnaire de démarrage), ou pendant le processus de démarrage, le serveur peut déclencher un arrêt immédiat.

Configuration de la détection de fuite du processeur

Configurez les alertes de sorte que les notifications requises soient générées et que des actions spécifiques soient lancées dans l'iDRAC en fonction de la gravité de la fuite du processeur.

1. Accédez à **Configuration** > **Paramètres système** > **Configuration des alertes** > **Alertes** > **Configuration des alertes** > **Système de refroidissement liquide**.
2. Cliquez sur **+**, puis cochez les cases **E-mail**, **Interruption SNMP**, **Alerte IPMI**, **Journal système distant**, **Événement WS**, **Journal du SE** et **Événement Redfish** pour les alertes critiques, d'avertissement et d'information.
3. Sélectionnez les actions (**Redémarrer, Cycle d'alimentation, Mettre hors tension**) dans la liste **Actions** pour les alertes critiques, d'avertissement et d'information.

Configuration de la détection de fuite au niveau du processeur graphique

Par défaut, l'alerte **Système de refroidissement liquide Action par défaut Mise hors tension** entraîne une **mise hors tension normale** en cas de fuite du processeur graphique dans le serveur. Vous pouvez configurer les options en fonction de vos besoins.

1. Accédez à **Configuration** > **Paramètres système** > **Configuration des alertes** > **Alertes** > **Configuration des alertes** > **Système de refroidissement liquide Action par défaut Mise hors tension**.
2. Cliquez sur **+**.
   Les cases **Gravité** et **Interruption SNMP** sont cochées. Dans la liste **Actions**, l'option **Mise hors tension normale** est sélectionnée par défaut.

   REMARQUE : Si le serveur ne parvient pas à effectuer une **mise hors tension progressive** dans un délai de 15 minutes, une mise hors tension forcée s'exécute.

   PRÉCAUTION : Si l'iDRAC redémarre et que la mise hors tension normale intervient simultanément, la mise hors tension du système prend plus de 20 minutes. Il est recommandé de forcer la mise hors tension du serveur et de ne pas attendre la fin de la mise hors tension normale.
3. Pour ajouter des notifications, cochez les cases **E-mail**, **Interruption SNMP**, **Alerte IPMI**, **Journal système distant**, **Événement WS**, **Journal du SE** et **Événement Redfish**.
4. Si vous souhaitez modifier l'action **Mise hors tension normale** par défaut, sélectionnez l'action **Aucune action** ou **Mise hors tension**.

REMARQUE : Si l'option **Aucune action** est choisie, le système ne s'arrête pas automatiquement en cas de fuite de liquide du processeur graphique.

15

Gestion des fichiers log

IDRAC fournit un journal Lifecycle qui contient les événements associés aux systèmes, périphériques de stockage, périphériques de réseau, mises à jour du firmware, modifications de la configuration, messages de licence, et ainsi de suite. Les événements système sont cependant également disponibles sous forme de journal distinct nommé SEL (System Event Log - Journal des événements système). Le journal Lifecycle est accessible via l'interface Web de l'iDRAC et de RACADM.

Lorsque la taille du journal Lifecycle atteint 800 Ko, les journaux sont compressés et archivés. Vous pouvez afficher uniquement les entrées des journaux non archivés 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.

Sujets :

Affichage du journal des événements système

Lorsqu'un événement système se produit sur un système géré, il est enregistré dans le journal des événements système (SEL). La même entrée SEL est également disponible dans le journal LC.

REMARQUE : Les journaux SEL et LC peuvent contenir des incohérences dans l'horodatage lors du redémarrage de l'iDRAC.

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 le journal SEL : `racadm clrsel`

Pour en savoir plus, voir Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Affichage du journal des événements système à l'aide de l'interface Web

Pour afficher le journal SEL, dans l'interface Web de l'iDRAC, accédez à **Maintenance** > **Journal des événements système**.

La page **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 de l'iDRAC**.

Cliquez sur **Enregistrer sous** pour enregistrer le journal **SEL** dans l'emplacement de votre choix.

REMARQUE : Si vous utilisez Internet Explorer et qu'un problème survient, téléchargez la mise à jour de sécurité cumulative pour Internet Explorer. Vous pouvez la télécharger à partir du site Web de support 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 le journal des événements système désactivé, une entrée est consignée dans le journal de Lifecycle Controller. Cette entrée inclut le nom d'utilisateur et l'adresse IP à partir de laquelle le journal SEL a été effacé.

Affichage du journal des événements système à l'aide de l'utilitaire de configuration d'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 de configuration de l'iDRAC. Pour ce faire, procédez comme suit :

1. Depuis l'utilitaire de configuration d'iDRAC, allez à **Journal des événements système**.
   La page **Paramètres iDRAC.Journal des événements système** affiche le **Nombre total d'enregistrements**.
2. Pour effacer les enregistrements, sélectionnez **Yes**. 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 relatives aux composants installés sur un système géré. Vous pouvez également ajouter des notes de travail à chaque entrée de journal.

Les événements et les activités suivantes sont consignés :

- Tous
- Intégrité du système : cette catégorie reprend l'ensemble des alertes associées au matériel du châssis du système.
- Intégrité du stockage : cette catégorie reprend les alertes associées au sous-système de stockage.
- Mises à jour : cette catégorie reprend les alertes générées en raison de mises à jour supérieures/inférieures de firmwares/pilotes.
- Audit : cette catégorie reprend le journal d'audit.
- Configuration : cette catégorie reprend les alertes associées aux modifications de configuration matérielle, logicielle et de firmware.
- Notes de travail

Lorsque vous vous connectez ou vous déconnectez d'iDRAC à l'aide de l'une des interfaces suivantes, les événements d'ouverture et de fermeture de session ou d'échec de la connexion sont consignés dans les journaux Lifecycle :

- SSH
- Interface web
- RACADM
- Redfish
- IPMI sur le LAN
- Série
- Console virtuelle
- Support virtuel

Vous pouvez afficher et filtrer les journaux en fonction de leur catégorie et de leur niveau de gravité. Vous pouvez également exporter une note de travail et l'ajouter à un événement de journal.

REMARQUE : La modification des journaux Lifecycle pour le mode de personnalité est générée uniquement au cours du démarrage à chaud de l'hôte.

Si vous lancez des travaux de configuration à l'aide de la CLI RACADM ou de l'interface web d'iDRAC, le journal Lifecycle contient les informations sur l'utilisateur, l'interface utilisée et l'adresse IP du système à partir duquel vous lancez le travail.

REMARQUE : Lorsqu'un événement se produit plusieurs fois, un seul journal d'événements s'affiche dans les journaux LC. Un journal supplémentaire (L0G007) s'affiche également pour indiquer le nombre de fois que cet événement s'est produit. Par défaut, les journaux d'événements en double sont désactivés dans l'iDRAC. Si vous souhaitez que tous les événements s'affichent dans les journaux LC, exécutez la commande RACADM `set idrac.logging.LCDuplicateEventEnable enabled`.

Affichage du journal Lifecycle à l'aide de l'interface Web

Pour afficher les journaux Lifecycle, cliquez sur **Maintenance** > **Journal Lifecycle**. La page **Journal Lifecycle** s'affiche. Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

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 de journal filtrées s'affichent dans les **Résultats du journal**.

Ajout de commentaires 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 visualiser les journaux Lifecycle, utilisez la commande `lclog`.

Pour en savoir plus, voir le *Guide de l'interface de ligne de commande RACADM d'iDRAC*.

Exportation des journaux du Lifecycle Controller

Vous pouvez exporter le journal de Lifecycle Controller complet (entrées actives et archivées) dans un seul fichier XML zippé vers un partage réseau ou vers le système local. Le fichier XML compressé porte l'extension `.xml.gz`. Les entrées de fichier sont classées par ordre séquentiel, du plus petit au plus grand numéro de séquence.

Exportation des journaux Lifecycle Controller via RACADM

Pour exporter les journaux Lifecycle Controller, utilisez la commande `lclog export`.

Pour en savoir plus, voir le *Guide de l'interface de ligne de commande RACADM d'iDRAC*.

Exportation des journaux du Lifecycle Controller à l'aide de 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 Controller vers un emplacement partagé du réseau.
- **Local** : exportez les journaux Lifecycle Controller vers un emplacement sur le système local.

REMARQUE : Lorsque vous indiquez les paramètres de partage réseau, il est conseillé d'éviter l'utilisation des caractères spéciaux dans le nom d'utilisateur et mot de passe ou de chiffrer en pourcentage les caractères spéciaux.

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

3. Cliquez sur **Exporter** pour exporter le journal sur un emplacement spécifié.

Empêcher le dépassement de capacité du journal Lifecycle

L'iDRAC permet d'empêcher le dépassement de capacité du journal Lifecycle à partir des consoles en raison de la forte fréquence de connexions à partir des consoles.

- Les événements USR0030/USR0032 sont consignés dans le journal Lifecycle pour chaque connexion/déconnexion réussie.
- Ces événements peuvent être agrégés dans un nouveau journal unique, en se basant sur un paramètre d'attribut.
- Un nouveau journal USR0036 doit être consigné dans le journal Lifecycle. Il contient une agrégation des événements de déconnexion et de connexion qui se sont produits pendant une durée spécifiée par l'attribut `LCLoggingAggregationTimeout`.

REMARQUE :

- Par défaut, l'attribut de fonctionnalité LCLogAggregation est désactivé.
- Par défaut, le délai d'expiration est défini sur 60 minutes et s'applique uniquement si LCLogAggregation est activé.

- USR0030 et USR0032 ne doivent pas être consignés dans le journal Lifecycle, mais continuent d'envoyer des alertes individuelles si les alertes correspondantes sont activées (SNMP/E-mail/Événement Redfish/WS-Event).

Ajout de notes de travail

Chaque utilisateur qui se connecte à l'iDRAC peut ajouter des notes de travail, qui sont stockées dans le journal de cycle de vie en tant qu'événement. Vous devez disposer de privilèges de journaux iDRAC pour ajouter des notes de travail. Chaque nouvelle note de travail prend en charge un maximum de 255 caractères.

REMARQUE : Vous ne pouvez pas supprimer une note de travail.

Pour ajouter une note de travail :

1. Dans l'interface Web de l'iDRAC, accédez à **Tableau de bord** > **Notes** > **ajouter une note**.
   La page **Notes de travail** s'affiche.
2. Dans **Notes de travail**, entrez le texte dans la zone de texte vide.

   REMARQUE : Il est conseillé de ne pas utiliser trop de caractères spéciaux.

3. Cliquez sur **Enregistrer**.
   La note de travail est ajoutée au journal. Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.

Affichage du journal Lifecycle

Les journaux Lifecycle Controller contiennent l'historique des modifications relatives aux composants installés sur un système géré. Vous pouvez également ajouter des notes de travail à chaque entrée de journal.

Les événements et les activités suivantes sont consignés :

- Tous
- Intégrité du système : cette catégorie reprend l'ensemble des alertes associées au matériel du châssis du système.
- Intégrité du stockage : cette catégorie reprend les alertes associées au sous-système de stockage.
- Mises à jour : cette catégorie reprend les alertes générées en raison de mises à jour supérieures/inférieures de firmwares/pilotes.
- Audit : cette catégorie reprend le journal d'audit.
- Configuration : cette catégorie reprend les alertes associées aux modifications de configuration matérielle, logicielle et de firmware.
- Notes de travail

Lorsque vous vous connectez ou vous déconnectez d'iDRAC à l'aide de l'une des interfaces suivantes, les événements d'ouverture et de fermeture de session ou d'échec de la connexion sont consignés dans les journaux Lifecycle :

- SSH
- Interface web
- RACADM
- Redfish
- IPMI sur le LAN
- Série
- Console virtuelle
- Support virtuel

Vous pouvez afficher et filtrer les journaux en fonction de leur catégorie et de leur niveau de gravité. Vous pouvez également exporter une note de travail et l'ajouter à un événement de journal.

REMARQUE : La modification des journaux Lifecycle pour le mode de personnalité est générée uniquement au cours du démarrage à chaud de l'hôte.

Si vous lancez des travaux de configuration à l'aide de la CLI RACADM ou de l'interface web d'iDRAC, le journal Lifecycle contient les informations sur l'utilisateur, l'interface utilisée et l'adresse IP du système à partir duquel vous lancez le travail.

REMARQUE : Lorsqu'un événement se produit plusieurs fois, un seul journal d'événements s'affiche dans les journaux LC. Un journal supplémentaire (L0G007) s'affiche également pour indiquer le nombre de fois que cet événement s'est produit. Par défaut, les journaux d'événements en double sont désactivés dans l'iDRAC. Si vous souhaitez que tous les événements s'affichent dans les journaux LC, exécutez la commande RACADM `set idrac.logging.LCDuplicateEventEnable enabled`.

Affichage du journal Lifecycle à l'aide de l'interface Web

Pour afficher les journaux Lifecycle, cliquez sur **Maintenance** > **Journal Lifecycle**. La page **Journal Lifecycle** s'affiche. Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

16

Surveillance et gestion de l'alimentation de l'iDRAC

Vous pouvez utiliser l'iDRAC pour surveiller et gérer la configuration requise de l'alimentation du système géré. Vous protégez ainsi le système contre les pannes de courant 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 fonctionnalité 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, disque de secours et correction du facteur de puissance.
- **Options de récupération de l'alimentation secteur** : configurez les options de récupération de l'alimentation afin que le système soit restauré en fonction de vos besoins.

Sujets :

Surveillance de l'alimentation

iDRAC surveille la consommation électrique du système en continu et affiche les valeurs d'alimentation suivantes :

- Seuils d'avertissement de consommation électrique et critiques.
- Valeurs de puissance cumulée, de puissance de crête et pic d'intensité de courant électrique.
- Consommation électrique au cours de la dernière heure, du dernier jour ou de la dernière semaine.
- Consommation électrique 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).

REMARQUE : L'histogramme de tendance de consommation électrique du système (horaire, quotidienne, hebdomadaire) est maintenu uniquement pendant que l'iDRAC est en cours d'exécution. Si l'iDRAC est redémarré, les données de consommation électrique existantes sont perdues et l'histogramme est redémarré.

REMARQUE : En mode HBM uniquement, l'alimentation de la mémoire HBM est prise en compte dans l'alimentation du package. Par conséquent, la lecture de la télémétrie de l'alimentation de la mémoire est signalée comme 0 pour ce mode.

REMARQUE : Après la mise à jour ou la réinitialisation du firmware iDRAC, le graphique de consommation électrique est effacé/réinitialisé.

Surveillance de l’indice de performances du processeur, de la mémoire et des modules d’entrée/sortie à l’aide de l’interface Web

Pour surveiller l’indice de performances du processeur, de la mémoire et des modules d’E/S, accédez à **Système** > **Performances** dans l’interface Web de l’iDRAC.

- Section **Performances système** : affiche la mesure actuelle et la mesure d’avertissement de l’UC, de l’indice d’utilisation de mémoire et d’E/S et de l’indice CUPS au niveau du système dans une vue graphique.
- Section **Historique de données des performances système** :
  - fournit les statistiques concernant l’utilisation du processeur, de la mémoire et des E/S et l’indice CUPS au niveau du système. Si le système hôte est mis hors tension, le graphique affiche la puissance hors ligne inférieure à 0 %.
  - Vous pouvez réinitialiser les valeurs maximales d’utilisation d’un capteur particulier. Cliquez sur **Réinitialiser les valeurs historiques maximales**. Vous devez disposer de privilèges de configuration pour réinitialiser la valeur maximale.
- Section **Mesures de performances** :
  - Afficher l’état et la valeur actuelle.
  - Affiche ou spécifie la limite d’utilisation de seuil d’avertissement. Vous devez disposer du privilège de configuration du serveur pour définir les valeurs de seuil.

Pour plus d’informations sur les propriétés affichées, voir l’**aide en ligne d’iDRAC**.

Surveillance de l'indice de performance de l'UC, de la mémoire et des modules d'E/S à l'aide de RACADM

Utilisez la sous-commande **SystemPerfStatistics** pour surveiller l'indice de performance de l'UC, de la mémoire et des modules d'E/S. Pour plus d’informations, rendez-vous sur le site Guide de la CLI RACADM de l’Integrated Dell Remote Access Controller.

Définition du seuil d’avertissement de consommation électrique

Vous pouvez définir la valeur du seuil d'avertissement du capteur de consommation électrique dans les systèmes en rack ou de type tour. Le seuil d'alimentation d'avertissement/critique pour les systèmes en rack et de type tour peut changer après un cycle d'alimentation du système, selon la capacité du PSU et la stratégie de redondance. Toutefois, le seuil d'avertissement ne doit pas dépasser le seuil critique, même si la capacité du PSU de la stratégie de redondance est modifiée.

Si vous effectuez une réinitialisation sur les valeurs par défaut, les seuils d’alimentation sont définis sur les paramètres par défaut.

Vous devez détenir le privilège de configuration pour définir la valeur du seuil d’avertissement du capteur de consommation électrique.

REMARQUE : La valeur par défaut du seuil d'avertissement est rétablie après l'exécution de la commande racreset ou une mise à jour de l'iDRAC.

Définition du seuil d’avertissement de consommation électrique à l’aide de l’interface Web

1. Dans l’interface Web de l’iDRAC, accédez à **Système** > **Présentation** > **Présentation de la consommation et des seuils d’alimentation**
2. Dans la section **Présentation de la consommation et des seuils d’alimentation**, cliquez sur **Modifier le seuil d’avertissement**. La page **Modifier le seuil d’avertissement** s’affiche.
3. Dans la colonne **Seuil d’avertissement**, saisissez la valeur en **Watts** ou en **BTU/h**.

   Les valeurs doivent être inférieures à celles des valeurs **de seuil d'échec**. Les valeurs sont arrondies à la valeur la plus proche divisible par 14. Si vous entrez **Watts**, le système calcule automatiquement et affiche la valeur **BTU/h**. De la même façon, si vous saisissez BTU/h, la valeur en **Watts** s’affiche.
4. Cliquez sur **Enregistrer**. Les valeurs sont configurées.

Exécution d’opérations de contrôle de l’alimentation

L’iDRAC permet d’exécuter à distance une mise sous tension, une mise hors tension, une réinitialisation, un arrêt normal, une ou un cycle d’alimentation à l’aide de l’interface Web ou RACADM.

Les opérations de contrôle de l’alimentation du serveur initiées à partir de l’iDRAC sont indépendantes du comportement du bouton d’alimentation configuré dans le BIOS. Vous pouvez utiliser la fonction PushPowerButton pour mettre le système hors tension/sous tension normalement, même si le BIOS est configuré pour ne rien faire lorsque le bouton d’alimentation physique est activé.

Exécution des opérations de contrôle de l’alimentation à l’aide de l’interface Web

Pour exécuter des opérations de contrôle d'alimentation :

1. Dans l’interface Web de l’iDRAC, accédez à **Configuration** > **Gestion de l’alimentation** > **Contrôle de l’alimentation**. Les options **Contrôle de l’alimentation** s’affichent.
2. Sélectionnez l'opération d'alimentation appropriée :
   - Mettre le système sous tension
   - Arrêter le système
   - 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 de l’iDRAC**.

Exécution d’opérations de contrôle de l’alimentation à l’aide de l’interface RACADM

Pour exécuter des actions d’alimentation, utilisez la commande **serveraction**.

Pour plus d’informations, rendez-vous sur le site Guide de la CLI RACADM de l’Integrated Dell Remote Access Controller.

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 applicative présente au datacenter. Il s’agit d’une fonctionnalité sous licence.

Affichage et configuration d'une stratégie de limitation de puissance

Lorsqu'une stratégie de seuil énergétique est activée, elle applique des limites de consommation définies par l'utilisateur sur le système. Si aucun seuil énergétique n’est activé, la politique de protection de la consommation du matériel par défaut est appliquée. Cette politique de protection de la consommation dépend de la stratégie définie par l’utilisateur. Les performances du système sont réglées de manière dynamique pour maintenir la consommation électrique entre les seuils définis.

La consommation électrique réelle dépend de la charge applicative. Elle peut momentanément dépasser le seuil, jusqu'à ce que les ajustements relatifs aux performances aient été effectués. Prenez par exemple un système affichant des consommations électriques minimum et maximum potentielles de 500 W et 700 W respectivement. Vous pouvez spécifier un seuil de bilan d’alimentation pour réduire la consommation à 525 W. Lorsque ce bilan d’alimentation est configuré, les performances du système sont ajustées de manière dynamique pour maintenir la consommation électrique de 525 W ou moins.

Si vous définissez un très faible seuil énergétique ou si la température ambiante est exceptionnellement élevée, la consommation électrique peut temporairement dépasser le seuil défini lorsque le système est en cours de mise sous tension ou en cours de réinitialisation.

Si la valeur de seuil énergétique est inférieure au seuil minimal recommandé, le contrôleur iDRAC peut ne pas pouvoir maintenir la limite demandée.

Vous pouvez définir la valeur en watts, BTU/h ou sous la forme d'un pourcentage de la limite de puissance maximum recommandée.

Lors de la définition du seuil énergétique en BTU/h, la conversion en watts est arrondie à la valeur entière la plus proche. Lorsque le système lit le seuil énergétique, la conversion de watts en BTU/h est également arrondie. En raison de l'arrondi, les valeurs réelles peuvent légèrement varier.

REMARQUE : La définition d'une limite de seuil énergétique à une valeur inférieure à la plage recommandée peut entraîner des performances variées, notamment une augmentation du temps de démarrage.

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 commande `set` :

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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 d'iDRAC, accédez à **Configuration** > **Gestion de l'alimentation** > **Stratégie de limitation de puissance**. La limite de la stratégie d'alimentation actuelle est affichée sous la section **Limites du seuil énergétique**.
2. Sélectionnez **Activer** sous **Seuil énergétique**.
3. Dans la section **Limites du seuil énergétique**, entrez la limite d'alimentation maximale comprise dans l'intervalle recommandé 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 d'alimentation à l'aide de 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 le bloc 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 **Règle de seuil d'alimentation.** Autrement, sélectionnez **Désactivé**.
3. Utilisez les paramètres recommandés, ou sous **Règle de seuil d'alimentation définie par l'utilisateur**, entrez les limites nécessaires.

   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 disque de secours et la correction de facteur de puissance.

REMARQUE : Les fonctionnalités de correction des disques de secours et du facteur de puissance peuvent ne pas être disponibles sur certaines plateformes/versions.

Le disque de secours est une fonction d'alimentation qui configure les unités d'alimentation redondante pour qu'elles se mettent hors tension en fonction de la charge du serveur. Ceci permet aux blocs 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 PSU, PSU1 ou PSU2 peut être configuré en tant que PSU principal.

Une fois le disque de secours activé, les PSU peuvent devenir actifs 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 PSU est activé. Un PSU est **actif** et fournit la majorité du courant ; l'autre PSU est en mode veille et fournit une petite partie du courant. Cette configuration de deux PSU et d'un disque de secours activé est souvent appelée 1 + 0. Si tous les PSU-1 se trouvent sur Circuit-A et que tous les PSU-2 se trouvent sur Circuit-B, et que le disque de secours est activé (configuration d'usine du disque de secours par défaut), Circuit-B a une charge très inférieure et déclenche les avertissements. Si le disque de secours est désactivé, le courant électrique est partagé à 50/50 entre les deux PSU, et le Circuit-A et le Circuit-B ont normalement la même charge.

Le facteur de puissance est le rapport de l'énergie consommée réelle sur la puissance 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 de puissance est activée lorsque le serveur est expédié depuis l'usine.

Configuration des options d'alimentation à l'aide de l'interface Web

Pour configurer les options d'alimentation :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Gestion de l'alimentation** > **Configuration de l'alimentation**.
2. Sous **Stratégie de redondance de l'alimentation**, sélectionnez les options requises. Pour en savoir plus, voir l'**Aide en ligne d'iDRAC**.
3. Cliquez sur **Appliquer**. Les options d'alimentation sont définies.

Configuration des options d'alimentation électrique à l'aide de l'interface RACADM

Pour configurer les options de bloc d'alimentation, utilisez les objets suivants avec la commande `get/set` :

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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 le bloc 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 disque de secours.
   - Définissez le bloc d'alimentation principale.
   - Activez ou désactivez la correction du 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 d'alimentation

Pour activer ou désactiver le bouton d'alimentation 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 d'alimentation ou **Désactivé** pour le désactiver.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres sont enregistrés.

Refroidissement Multi-Vector

Le refroidissement multivecteur met en œuvre une approche multibroche en matière de régulations thermiques dans les plateformes de serveur Dell. Vous pouvez configurer les options de refroidissement multivecteur via l'interface Web de l'iDRAC en accédant à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Configuration du refroidissement**. Il comprend (mais pas exclusivement) :

- Vaste ensemble de capteurs (thermiques, d'alimentation, d'inventaire, etc.) qui permet d'interpréter avec précision l'état thermique du système en temps réel à différents emplacements du serveur. Il n'affiche qu'un sous-ensemble restreint de capteurs correspondant aux besoins des utilisateurs en fonction de la configuration.
- Un algorithme de contrôle en circuit fermé intelligent et adaptatif optimise la réponse des ventilateurs afin de maintenir les températures des composants. Il préserve également l'alimentation du ventilateur, l'utilisation de la circulation d'air et l'acoustique.
- L'utilisation de l'adressage de zones du ventilateur permet de lancer le refroidissement lorsque cela est nécessaire. Par conséquent, il en résulte des performances maximales sans compromettre l'efficacité de l'utilisation de l'alimentation.
- Représentation exacte de la circulation d'air d'une carte PCIe dans chaque logement sous forme de valeur LFM (pieds linéaires par minute) (une norme de l'industrie acceptée relative à la spécification des besoins de circulation d'air d'une carte PCIe). L'affichage de cette mesure dans diverses interfaces iDRAC permet à l'utilisateur de :
  - Connaître la capacité LFM maximale de chaque logement du serveur.
  - Connaître l'approche adoptée pour le refroidissement PCIe de chaque logement (circulation d'air contrôlée, température contrôlée).
  - Connaître la capacité LFM minimale fournie dans un logement, si la carte est une carte tierce (carte personnalisée définie par l'utilisateur).
  - entrer une valeur LFM minimale personnalisée pour la carte tierce, ce qui permet de mieux définir les besoins de refroidissement de la carte dont l'utilisateur est mieux informé par le biais de la spécification de carte personnalisée.
- Affiche en temps réel la mesure de la circulation d'air (CFM, pieds cubes par minute) dans différentes interfaces de l'iDRAC à l'utilisateur afin de permettre un équilibrage de la circulation d'air du datacenter en fonction de l'agrégation de la consommation CFM par serveur.
- Permet des paramètres thermiques personnalisés, tels que les profils thermiques (Performances maximales ou Performances maximales par Watt, Plafond acoustique), les options de vitesse du ventilateur personnalisées (vitesse minimale du ventilateur, décalages de vitesse du ventilateur) et les paramètres de température d'évacuation personnalisés.
  - La plupart de ces paramètres permettent un refroidissement supplémentaire par rapport au refroidissement de base généré par les algorithmes thermiques et empêchent les vitesses du ventilateur de devenir inférieures aux besoins de refroidissement du système.

    REMARQUE : La seule exception est lorsque des vitesses de ventilateur sont ajoutées pour des cartes PCIe tierces. La circulation d'air fournie par l'algorithme thermique pour les cartes tierces peut être supérieure ou inférieure aux besoins de refroidissement réels de la carte et l'utilisateur peut régler la réponse pour la carte en entrant la valeur LFM correspondant à la carte tierce.

  - L'option Température d'évacuation personnalisée limite la température d'évacuation aux paramètres souhaités par le client.

    REMARQUE : Il est important de noter qu'avec certaines configurations et charges applicatives, il peut ne pas être physiquement possible de réduire l'évacuation au-dessous d'un point défini souhaité (par ex., paramètre d'évacuation personnalisé de 45 °C avec une température d'entrée élevée {par ex. 30 °C} et une configuration chargée {haute consommation électrique du système, circulation d'air faible}).

  - Plafond acoustique est une nouvelle option dans le serveur PowerEdge de 14e génération. Elle limite la consommation électrique du CPU et contrôle la vitesse du ventilateur et le plafond acoustique. Cela concerne uniquement les déploiements acoustiques et peut entraîner une réduction des performances système.
- La disposition et la conception du système permettent une meilleure capacité de circulation d'air (en permettant une alimentation élevée) et des configurations système denses. Elle limite les restrictions système et augmente la densité des fonctions.

- La rationalisation de la circulation d'air permet d'obtenir un rapport circulation d'air/consommation électrique du ventilateur efficace.
- Les ventilateurs personnalisés sont conçus pour une efficacité accrue, de meilleures performances, une durée de vie plus longue et moins de vibrations. Ils permettent également d'obtenir un meilleur résultat acoustique.
  - La durée de vie moyenne d'un ventilateur de serveur varie en fonction des spécifications de la plateforme.
  - Si un ventilateur est retiré ou inséré à chaud, il peut s'écouler jusqu'à 90 secondes avant que les interfaces de l'iDRAC reflètent les modifications sur la page **Refroidissement** (**Système** > **Présentation** > **Refroidissement** > **Ventilateurs**).
- Les dissipateurs de chaleur personnalisés sont conçus pour optimiser le refroidissement des composants à la circulation d'air minimale (requise) tout en prenant en charge des processeurs graphiques hautes performances.

Configuration de la récupération de l'alimentation secteur

Vous pouvez configurer l'état d'alimentation attendu après une perte et une récupération de l'alimentation du serveur.

1. Sélectionnez l'état attendu du serveur dans le champ **Récupération de l'alimentation secteur** après la récupération de l'alimentation. L'option par défaut est **Activé**.

   REMARQUE : Sélectionnez **Dernier** si vous souhaitez restaurer le serveur à son état avant que la perte d'alimentation n'ait eu lieu.

2. Sélectionnez l'option **Délai de récupération d'alimentation secteur** en fonction du moment où vous souhaitez mettre le serveur sous tension.
3. Si vous avez défini **Délai de récupération d'alimentation secteur** sur **Défini par l'utilisateur**, saisissez le délai en secondes **Délai défini par l'utilisateur (120 s à 600 s)** (entre 120 et 600 secondes).

17

Mises à jour directes d’iDRAC

L’iDRAC offre la possibilité hors bande de mettre à jour le firmware de divers composants d’un serveur PowerEdge. La mise à jour directe de l’iDRAC permet d’éliminer les tâches intermédiaires lors des mises à jour. Seuls les fonds de panier SEP (passifs) sont pris en charge pour les mises à jour directes.

Auparavant, l’iDRAC effectuait des mises à jour échelonnées pour lancer la mise à jour de firmware des composants. À partir de cette version, les mises à jour directes sont appliquées au bloc d'alimentation et au fond de panier. En utilisant les mises à jour directes, le bloc d'alimentation et le fond de panier disposent de mises à jour plus rapides. Pour le bloc d’alimentation, il n’est pas nécessaire d’effectuer un redémarrage (pour initialiser les mises à jour) et la mise à jour peut s’effectuer lors d’un redémarrage unique.

Grâce à la fonctionnalité de mise à jour directe de l’iDRAC, vous pouvez supprimer le premier redémarrage pour lancer les mises à jour. Le deuxième redémarrage est contrôlé par l’appareil lui-même et l’iDRAC avertit l’utilisateur si une réinitialisation distincte est nécessaire via l’état de la tâche.

REMARQUE : Pour toute mise à jour nécessitant une réinitialisation/un redémarrage de l’iDRAC ou si l’iDRAC est redémarré, il est recommandé de vérifier si l’iDRAC est prêt en attendant quelques secondes, avec un délai d’expiration maximum de 5 minutes, avant d’utiliser une autre commande.

18

Configuration, surveillance et inventaire des périphériques réseau

Vous pouvez inventorier, surveiller et configurer les périphériques réseau suivants :

- Cartes d'interface réseau (NIC)
- Adaptateurs réseau de convergence (CNA)
- Cartes LOM (LAN On Motherboard)
- Carte OCP (Open Compute Project)

Avant de désactiver NPAR ou une partition individuelle sur les périphériques CNA, assurez-vous d'effacer tous les attributs d'identité d'E/S (par exemple : adresse IP, adresses virtuelles, initiateur et cibles de stockage) et les attributs au niveau de la partition (par exemple : allocation de bande passante). Vous pouvez désactiver une partition en modifiant le paramètre d'attribut VirtualizationMode sur NPAR ou en désactivant toutes les personnalités d'une partition.

Selon le type de périphérique CNA installé, les paramètres des attributs de partition utilisés la dernière fois que la partition était active peuvent ne pas être conservés. Lorsque vous activez une partition, définissez tous les attributs d'identité d'E/S ainsi que les attributs liés à la partition. Vous pouvez activer une partition en modifiant le paramètre d'attribut VirtualizationMode sur NPAR ou en activant une personnalité (par exemple : NicMode) sur la partition.

Sujets :

Inventaire et surveillance des périphériques HBA FC

Vous pouvez surveiller à distance l'intégrité et afficher l'inventaire des périphériques HBA FC dans le système géré. Les HBA FC Emulex et QLogic sont pris en charge. Pour chaque périphérique HBA FC, vous pouvez afficher les informations suivantes sur les ports :

- Informations de cible de stockage FC
- Informations de cible de stockage NVMe
- Propriétés du port
- Statistiques de réception et de transmission

REMARQUE : Les adaptateurs HBA Emulex FC8 ne sont pas pris en charge.

Surveillance des périphériques HBA FC à l'aide de RACADM

Pour afficher les informations sur les périphériques HBA FC à l'aide de RACADM, utilisez la commande `hwinventory`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Surveillance des périphériques HBA FC à l'aide de l'interface Web

Pour afficher les informations du périphérique HBA FC à l'aide de l'interface Web, accédez à **Système** > **Présentation** > **Périphériques réseau** > **Fibre Channel**. Pour plus d'informations sur les propriétés affichées, voir l'**aide en ligne de l'iDRAC**.

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.

Inventaire et surveillance des périphériques réseau

Vous pouvez surveiller à distance l'intégrité et afficher l'inventaire des périphériques réseau dans le système géré.

Dans le cas de chaque périphérique, vous pouvez afficher les informations suivantes sur les ports et les partitions activées :

- Condition de la liaison
- Propriétés
- Paramètres et fonctionnalités
- Statistiques de réception et de transmission
- iSCSI, initiateur FCoE et informations de la cible

REMARQUE : Dans le cas d'un appareil NIC intégré, la représentation du BIOS de chaque port LOM est considérée comme un périphérique de carte NIC individuel, de sorte que la chaîne FQDD s'affiche en tant que **Carte NIC intégrée 1 Port 1 Partition 1** et **Carte NIC intégrée 2 Port 1 Partition 1.**

Surveillance des périphériques réseau à l'aide de RACADM

Pour afficher des informations sur les périphériques réseau, utilisez les commandes `hwinventory` et `nicstatistics`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

D'autres propriétés peuvent s'afficher lors de l'utilisation de RACADM en plus des propriétés affichées dans l'interface Web de l'iDRAC.

Surveillance des périphériques réseau à l'aide de l'interface Web

Pour afficher les informations du périphérique réseau à l'aide de l'interface Web, accédez à **Système** > **Présentation** > **Appareils réseau**. La page **Périphériques réseau** s'affiche. Pour plus d'informations sur les propriétés affichées, voir l'**aide en ligne de l'iDRAC**.

REMARQUE : La propriété de port **Wake-on-LAN** pour les appareils réseau dans l'interface utilisateur de l'iDRAC peut contenir des données obsolètes, car elles sont mises à jour lors du CSIOR. Reportez-vous à la sortie RACADM pour connaître les données correctes de cette propriété.

Vue de connexion

La vérification et le dépannage manuels des connexions réseau des serveurs ne sont pas gérables dans un environnement de datacenter. L'iDRAC rationalise cette tâche avec la vue Connexion de l'iDRAC. Cette fonctionnalité vous permet de vérifier et dépanner les connexions réseau à distance à partir de la même interface uilisateur graphique centralisée que vous utilisez pour le déploiement, la mise à jour, la surveillance et la maintenance des serveurs. Dans l'iDRAC, Vue de connexion fournit les détails de l'adressage physique des ports du commutateur aux ports réseau du serveur et aux connexions des ports dédiés à l'iDRAC. Toutes les cartes réseau prises en charge sont visibles dans Vue de connexion, quelle que soit la marque.

Au lieu de vérifier et de dépanner manuellement les connexions réseau du serveur, vous pouvez afficher et gérer les connexions des câbles réseau à distance.

La vue de connexion fournit des informations sur les ports de commutateur qui sont connectés aux ports de serveur et au port dédié iDRAC. Les ports réseau du serveur incluent le port LOM PowerEdge, ceux des cartes OCP, des cartes mezzanine et des cartes d'extension PCIe.

Pour afficher la vue de connexion des périphériques réseau, accédez à **Système** > **Présentation** > **Périphériques réseau** > **Vue de connexion**.

En outre, vous pouvez cliquer sur **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Paramètres communs** > **Vue de connexion** pour activer ou désactiver la vue de connexion.

Vue Connexion peut être explorée avec la commande `SwitchConnection View` RACADM.

Activé	Sélectionnez **Activé** pour activer Vue de connexion. Par défaut, l'option **Activé** est sélectionnée.

État	Affiche **Activé**, si vous activez l'option de vue de connexion à partir de **Vue de connexion** dans les paramètres iDRAC.
ID de connexion de commutateur	Affiche l'ID du châssis LLDP du commutateur via lequel le port de l'appareil est connecté.
ID de connexion du port du commutateur	Affiche l'ID de port LLDP du port du commutateur auquel le port de l'appareil est connecté.

REMARQUE : L'ID de connexion du commutateur et l'ID de connexion du port de commutateur sont disponibles une fois la vue de connexion activée et le lien connecté. La carte réseau associée doit être compatible avec la vue de connexion. Seuls les utilisateurs disposant de privilèges de configuration iDRAC peuvent modifier les paramètres de la Vue de connexion.

L'iDRAC prend en charge l'envoi de paquets LLDP standard aux commutateurs externes. Cela fournit des options pour découvrir les iDRAC sur le réseau. L'iDRAC envoie deux types de paquets LLDP au réseau sortant :

- **Topologie LLDP** : dans cette fonctionnalité, le paquet LLDP passe par tous les ports NIC du serveur pris en charge afin qu'un commutateur externe puisse localiser le serveur d'origine, le port OCP [NIC FQDD], l'emplacement du module d'E/S dans le châssis, etc. La fonctionnalité Topologie LLDP est disponible en option pour tous les serveurs PowerEdge. Les paquets LLDP contiennent des informations relatives à la connectivité du périphérique réseau du serveur et sont utilisées par les modules d'E/S et les commutateurs externes pour mettre à jour leur configuration.

  REMARQUE : La topologie LLDP n'est pas prise en charge sur les contrôleurs 1 GbE et sélectionne les contrôleurs 10 GbE (Intel X520, QLogic 578xx).

- **LLDP de découverte** : dans cette fonctionnalité, le paquet LLDP ne passe que par le port actif NIC iDRAC utilisé (dédié NIC ou LOM partagé), de sorte qu'un commutateur adjacent peut localiser le port de connexion iDRAC dans le commutateur. La fonctionnalité LLDP de découverte est spécifique uniquement au port réseau iDRAC actif et ne sera pas visible sur tous les ports réseau du serveur. La fonctionnalité Découverte LLDP contient certains détails de l'iDRAC, tels que l'adresse IP, l'adresse MAC, le numéro de série, etc. Le commutateur peut détecter automatiquement les appareils iDRAC qui y sont connectés et certaines données de l'iDRAC.

  REMARQUE : Si l'adresse MAC virtuelle est effacée sur un port/une partition, celle-ci est identique à l'adresse MAC.

Pour activer ou désactiver la fonctionnalité Topologie LLDP, accédez à **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Paramètres communs** > **Topologie LLDP**.

Pour activer ou désactiver la LLDP de découverte iDrac, accédez à **Paramètres iDRAC** > **Connectivité** > **Réseau** > **Paramètres communs** > **LLDP de découverte iDrac**. Par défaut, l'option Enable (activation) est sélectionnée.

Vous pouvez afficher le paquet LLDP émis par l'iDRAC à partir du commutateur à l'aide de la commande : `show lldp neighbors`.

Actualiser la vue de connexion

Utilisez **Actualiser la vue de connexion** pour obtenir les dernières informations de l'ID de connexion du commutateur et de l'ID de connexion du port de switch.

REMARQUE : Si l'iDRAC dispose d'informations sur la connexion du commutateur et la connexion du port du commutateur pour le port réseau du serveur ou le port réseau de l'iDRAC. Si les informations sur la connexion du commutateur et la connexion du port du commutateur ne sont pas actualisées pendant cinq minutes, ces informations s'affichent comme des données obsolètes (dernières données correctes connues) pour toutes les interfaces utilisateur.

Vue de connexion : valeurs possibles

Fonction désactivée	La fonction Vue de connexion est désactivée. Pour afficher les données de la vue de connexion, activez la fonction.
Aucune liaison	Indique que la liaison associée au port de contrôleur réseau est hors service.
Non disponible	LLDP n'est pas activé sur le commutateur. Vérifiez si LLDP est activé sur le port de switch.
Non pris en charge	Le contrôleur réseau ne prend pas en charge la fonction Vue de connexion.
Données obsolètes	Dernières données fiables connues. Soit la liaison du port du contrôleur réseau est en panne ou le système est hors tension. Utilisez l'option d'actualisation pour actualiser les détails de la vue de connexion afin d'obtenir les données les plus récentes.

Données valides	Affiche les informations d'ID de connexion du port de switch et d'ID de connexion du commutateur valides.

Inventaire et surveillance des émetteurs-récepteurs SFP

Vous pouvez surveiller à distance l'intégrité et afficher l'inventaire des émetteurs-récepteurs SFP connectés au système. Vous trouverez ci-dessous les émetteurs-récepteurs pris en charge :

- SFP
- SFP+
- SFP28
- SFP-DD
- QSFP
- QSFP+
- QSFP28
- QSFP-DD
- Modules base-T
- Câbles AOC & DAC
- Base-T RJ-45 connectée à l'Ethernet
- Fibre Channel
- Ports d'adaptateur IB

Les informations les plus utiles concernant les émetteurs-récepteurs sont le numéro de série et le numéro de référence de l'EPROM de l'émetteur-récepteur. Ils permettent de vérifier les émetteurs-récepteurs installés à distance lors du dépannage des problèmes de connectivité. Pour chaque émetteur-récepteur SFP, vous pouvez afficher les informations suivantes sur les ports :

- Nom du fournisseur
- Numéro de référence
- Révision
- Numéro de série
- ID de l'appareil
- Type d'interface

Surveillance des émetteurs-récepteurs SFP à l'aide de l'interface Web

Pour afficher les informations d'un émetteur-récepteur SFP à l'aide de l'interface Web, accédez à **Système** > **Présentation** > **Périphériques réseau**, puis cliquez sur un périphérique particulier. Pour plus d'informations sur les propriétés affichées, voir l'**aide en ligne de l'iDRAC**.

Le nom de la page affiche également le numéro du logement dans lequel l'émetteur-récepteur est disponible sous Statistiques des ports.

Les données de surveillance des appareils SFP sont uniquement disponibles pour les SFP actifs. Les informations suivantes s'affichent :

- Puissance de sortie de l'émetteur
- Courant de polarisation de l'émetteur
- Puissance d'entrée du récepteur
- Tension Vcc
- Température

Surveillance des émetteurs-récepteurs SFP à l'aide de RACADM

Pour afficher les informations des émetteurs-récepteurs SFP à l'aide de RACADM, utilisez la commande `networktransceiverstatistics`.

Pour en savoir plus, voir le *Guide de la CLI RACADM de l'iDRAC (Integrated Dell Remote Access Controller)*.

Streaming de la télémétrie

La télémétrie permet aux utilisateurs de collecter et de transmettre en temps réel des événements, des journaux de données et des métriques d'appareil d'un serveur PowerEdge vers une application client ou serveur externe inscrite. À l'aide de la télémétrie, vous pouvez définir le type et la fréquence des rapports qui doivent être générés.

REMARQUE : Cette fonctionnalité est prise en charge sur toutes les plateformes et nécessite une licence iDRAC Datacenter.

La télémétrie est une solution un à plusieurs pour la collecte et le streaming des données du système d'un ou plusieurs serveurs PowerEdge (iDRAC) vers un service centralisé de « surveillance, analyse et alerte de serveurs distants ». La fonctionnalité prend également en charge la collecte de données à la demande.

Les données de télémétrie incluent les métriques/l'inventaire et les journaux/événements. Les données peuvent être diffusées (transmises) ou collectées (extraites) de l'iDRAC vers ou par des consommateurs distants tels que le client Redfish et le serveur Syslog distant. Les données de télémétrie sont également fournies au contrôleur de données SupportAssist iDRAC à la demande. La collecte de données et le rapport sont basés sur des définitions prédéfinies de métriques, de déclencheurs et de rapport de télémétrie Redfish. Les paramètres de streaming de télémétrie peuvent être configurés via l'interface web d'iDRAC, RACADM, Redfish et le profil de configuration de serveur (SCP).

Pour activer la télémétrie, accédez à **Configuration** > **Paramètres système** > **Analyse des données de télémétrie** et sélectionnez **Activé** dans la liste **Flux de données de télémétrie**. Le streaming de données est automatique jusqu'à l'activation de la télémétrie.

Le tableau suivant décrit les rapports de métriques qu'il est possible de générer à l'aide de la télémétrie :

Tableau 35. Rapport de métriques

Type	Groupe de métriques	Inventaire	Capteur	Statistiques	Configuration	Mesures
Périphériques d'E/S	Cartes NIC	Non	Oui	Oui	Non	Non
	FC HBA	Non	Oui	Oui	Non	Non
Serveur - Périphériques	CPU	Non	Oui	Non	Non	Oui
	Mémoire	Non	Oui	Non	Non	Oui
	Ventilateurs	Non	Oui	Non	Non	Non
	Unités d'alimentation	Non	Non	Non	Non	Oui
	Capteurs	Non	Oui	Non	Non	Non
Spécifications environnementales	Caractéristiques thermiques	Non	Oui	Non	Non	Oui
	Alimentation	Non	Non	Oui	Non	Oui
	Performances	Non	Non	Oui	Non	Non
Accélérateurs	Processeurs graphiques	Non	Non	Oui	Non	Oui

Pour connaître les descriptions des champs de la section Télémétrie, voir l'**Aide en ligne de l'iDRAC**.

REMARQUE :

- Lorsque le fond de panier SAS/SATA est connecté au contrôleur SATA intégré, il est probable que le fond de panier ne s'affiche pas en tant que boîtier dans le système et ne s'affiche pas non plus dans l'inventaire du matériel.
- StorageDiskSMARTDATA est uniquement pris en charge sur les disques SSD avec protocole de bus SAS/SATA et derrière le contrôleur BOSS.
- Les données StorageSensor sont signalées uniquement pour les disques en mode Prêt/En ligne/Non RAID et non derrière le contrôleur BOSS.
- NVMeSMARTData est uniquement pris en charge pour les disques SSD (PCIeSSD/NVMe Express) avec protocole de bus PCIe (et non derrière SWRAID) et aussi derrière le contrôleur BOSS-N1.
- Les données GPGPUStatistics sont uniquement disponibles dans des modèles GPGPU spécifiques prenant en charge la fonctionnalité de mémoire ECC.

- PSUMetrics n'est pas disponible sur les plates-formes modulaires.
- Les mesures d'alimentation des ventilateurs et des PCIe peuvent afficher 0 pour certaines plates-formes.
- Le rapport CUPS a été renommé SystemUsage dans la version 4.40.00.00 ; il est pris en charge sur les plateformes INTEL et AMD.

Workflow de télémétrie :

1. Installez la licence Datacenter, si ce n'est déjà fait.
2. Configurez les paramètres de télémétrie globaux, notamment l'activation de la télémétrie, ainsi que l'adresse et le port du réseau du serveur Rsyslog à l'aide de l'interface utilisateur RACADM, Redfish, SCP ou iDRAC.
3. Configurez les paramètres de streaming du rapport de télémétrie suivants sur le rapport ou le journal de périphérique requis à l'aide de l'interface RACADM ou Redfish :
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

   REMARQUE : Activez les alertes iDRAC et les événement Redfish pour le matériel spécifique pour lequel vous avez besoin de rapports de télémétrie.
4. Le client Redfish envoie une demande d'abonnement à Redfish EventService sur l'iDRAC.
5. L'iDRAC génère et transmet le rapport de métrique ou les données de journal/événement au client abonné lorsque les conditions de déclenchement prédéfinies sont remplies.

Contraintes liées aux fonctionnalités :

1. Pour des raisons de sécurité, l'iDRAC prend uniquement en charge la communication HTTPS sur le client.
2. Pour des raisons de stabilité, l'iDRAC prend en charge jusqu'à huit abonnements.
3. La suppression des abonnements est prise en charge via l'interface Redfish uniquement, même pour la suppression manuelle par l'administrateur.

Comportement de la fonctionnalité de télémétrie :

- L'iDRAC génère et transmet (HTTP POST) le rapport de métrique ou les données de journal/événement à tous les clients abonnés vers la destination spécifiée dans l'abonnement lorsque les conditions de déclenchement prédéfinies sont remplies. Les clients reçoivent les nouvelles données uniquement après la création réussie de l'abonnement.
- Les données de métrique incluent l'horodatage au format ISO, heure UTC (se termine par « Z »), au moment de la collecte de données à partir de la source.
- Les clients peuvent mettre fin à un abonnement en envoyant un message HTTP DELETE à l'URI de la ressource d'abonnement via l'interface Redfish.
- Si l'abonnement est supprimé par l'iDRAC ou par le client, l'iDRAC n'envoie pas de rapport (HTTP POST). Si le nombre d'erreurs de livraison dépasse les seuils prédéfinis, l'iDRAC peut supprimer un abonnement.
- Si un utilisateur dispose de privilèges administrateur, il peut supprimer les abonnements, mais uniquement via l'interface Redfish.
- L'iDRAC informe le client de la résiliation d'un abonnement en envoyant l'événement « Abonnement résilié » comme dernier message.
- Les abonnements sont persistants et peuvent rester même après le redémarrage de l'iDRAC. Cependant, vous pouvez supprimer les abonnements en effectuant des opérations `racresetcfg` ou `racadm systemerase idrac`.
- Les interfaces utilisateur comme RACADM, Redfish, SCP et iDRAC affichent l'état actuel des abonnements client.
- La préparation du service de télémétrie peut être vérifiée à l'aide d'un nouvel attribut `TelemetryServiceStatus` ajouté sous l'appel d'API `GetRemoteServiceAPIStatus`. Cet attribut est ajouté à la liste existante de LTStatus, RTStatus, ServerStatus et Status.

Définition du rapport métrique

Une définition du rapport de mesures permet de définir l'ensemble des mesures qui doivent figurer dans un rapport de télémétrie et la manière dont le rapport doit être généré et diffusé.

Le streaming de télémétrie iDRAC génère des mesures qui peuvent fournir des données sur l'état du serveur sans compromettre les performances du serveur principal. Ces mesures incluent divers paramètres système tels que l'utilisation du processeur, l'utilisation de la mémoire, la consommation électrique, les relevés de température, la vitesse du ventilateur, etc.

Importer et modifier la définition du rapport de mesures

Pour personnaliser une définition du rapport de mesures en fonction de vos besoins, importez la définition et modifiez ses propriétés.

1. Accédez à **Configuration** > **Paramètres système** > **Configuration de la télémétrie** > **Définition du rapport de mesures**.
2. Sélectionnez le **Type d'emplacement**.
3. Cliquez sur **Choisir un fichier** et sélectionnez le fichier.
4. Cliquez sur **Importer**.
   Le fichier de rapport de mesures est importé. Le rapport s'affiche dans la liste **Rapports de télémétrie**.
5. Si vous souhaitez modifier un rapport de mesures spécifique, cliquez sur **Actions** > **Modifier les propriétés du rapport** pour ce rapport.
   La boîte de dialogue **Paramètres de rapport** s'affiche.
6. Modifiez les paramètres de rapport et cliquez sur **Enregistrer**.

Exporter la définition du rapport de mesures

Exportez la définition du rapport de mesures si vous souhaitez comparer les performances des serveurs ou utiliser le rapport de mesures comme modèle pour d'autres serveurs.

1. Accédez à **Configuration** > **Paramètres système** > **Configuration de la télémétrie** > **Définition du rapport de mesures**.
2. Sélectionnez le **Type d'emplacement**.
3. Sélectionnez la **Définition du rapport de mesures**.
4. Cliquez sur **Enregistrer**.
   Le fichier de rapport de mesures est enregistré.

Déclencheurs

Les déclencheurs de télémétrie définissent un ensemble de conditions. Les rapports de mesures associés sont générés et diffusés en continu en fonction de ces conditions. Les conditions peuvent inclure un événement système ou une condition définie par l'utilisateur, telle qu'une mesure dépassant un seuil ou atteignant une valeur donnée.

Les déclencheurs peuvent être configurés pour surveiller un large éventail de conditions, telles que les pannes matérielles, les modifications des performances du système ou d'autres événements importants. L'iDRAC envoie le rapport de mesures associé à l'aide de l'une des méthodes de streaming configurées. Ces méthodes sont Server-Sent Events (SSE) ou Post to Subscription.

Exporter les déclencheurs

Exportez les déclencheurs pour comparer les déclencheurs des serveurs ou utiliser le déclencheur comme modèle pour d'autres serveurs.

1. Accédez à **Configuration** > **Paramètres système** > **Configuration de la télémétrie** > **Déclencheurs**.
2. Sélectionnez le **Type d'emplacement**.
3. Sélectionnez le déclencheur dans la liste **Nom de fichier**.
4. Cliquez sur **Exporter**.
   Le fichier des déclencheurs s'affiche dans la liste **Déclencheurs**.

Importer les déclencheurs

Si vous souhaitez personnaliser un déclencheur en fonction de vos besoins, importez-le.

1. Accédez à **Configuration** > **Paramètres système** > **Configuration de la télémétrie** > **Déclencheurs**.
2. Sélectionnez le **Type d'emplacement**.
3. Cliquez sur **Choisir un fichier** et sélectionnez le fichier.
4. Cliquez sur **Importer**.
   Le fichier du déclencheur est importé. Le déclencheur s'affiche dans la liste **Déclencheurs**.

Capture de données série

L'iDRAC vous permet de capturer les données série de redirection de la console pour une récupération ultérieure à l'aide de la fonctionnalité de capture de données série. Cette fonctionnalité nécessite une licence iDRAC Datacenter.

L'objectif de la fonctionnalité de capture des données série est de capturer les données série du système et de les stocker afin que le client puisse les récupérer ultérieurement à des fins de débogage.

Vous pouvez activer ou désactiver une capture de données série à l'aide des interfaces RACADM, Redfish et de l'iDRAC. Lorsque cet attribut est activé, l'iDRAC capture le trafic série reçu sur l'appareil série hôte Device2, quels que soient les paramètres du mode MUX série.

Pour activer ou désactiver la capture de données série à l'aide de l'interface utilisateur de l'iDRAC, accédez à la page **Maintenance** > **Diagnostics** > **Journaux de données série**, puis cochez la case pour activer/désactiver.

REMARQUE :

- Cet attribut persiste au redémarrage de l'iDRAC.
- La réinitialisation du firmware à la valeur par défaut désactive cette fonctionnalité.
- Quand la capture des données série est activée, la mémoire tampon continue de s'ajouter aux données récentes. Si l'utilisateur désactive la capture série et l'active à nouveau, l'iDRAC commence à ajouter la dernière mise à jour.

La capture des données série du système démarre lorsque l'utilisateur active la balise de capture des données série à partir de n'importe quelle interface. Si la capture de données série est activée après le démarrage du système, vous devez redémarrer le système pour que le BIOS puisse voir le nouveau paramètre (redirection de console activée demandée par l'iDRAC) pour obtenir les données série. L'iDRAC démarre la capture des données en continu et les stocke dans la mémoire partagée avec une limite de 512 Ko. Cette mémoire tampon est circulaire.

REMARQUE :

- Pour que cette fonctionnalité soit opérationnelle, vous devez disposer des privilèges de connexion et de contrôle du système.
- Cette fonctionnalité nécessite une licence iDRAC Datacenter.

Configuration dynamique des adresses virtuelles, de l'initiateur et de la cible de stockage

Vous pouvez afficher et configurer de manière dynamique les paramètres d'adresse virtuelle, d'initiateur et de stockage cible, et appliquer une stratégie de persistance. L'application peut ainsi appliquer les paramètres en fonction des changements d'état d'alimentation (c'est-à-dire le redémarrage du système d'exploitation, la réinitialisation à chaud, la réinitialisation à froid ou le cycle CA), mais aussi en fonction du paramètre de la stratégie de persistance correspondant à cet état d'alimentation. Cela offre une plus grande flexibilité dans les déploiements qui nécessitent une reconfiguration rapide des charges applicatives système vers un autre système.

Les adresses virtuelles sont les suivantes :

- Adresse MAC virtuelle
- Adresse MAC iSCSI virtuelle
- Adresse MAC FIP virtuelle
- WWN virtuel
- WWPN virtuel

REMARQUE : Lorsque vous désactivez la stratégie de persistance, toutes les adresses virtuelles sont réinitialisées à l'adresse permanente par défaut définie en usine.

REMARQUE : Certaines cartes dotées d'attributs FIP virtuel, WWN virtuel et MAC WWPN virtuel, d'attributs MAC WWPN et WWN virtuels sont configurées automatiquement lorsque vous configurez le FIP virtuel.

À l'aide de la fonction d'identité d'E/S, vous pouvez :

- Afficher et configurer les adresses virtuelles pour les périphériques réseau et Fibre Channel (par exemple, NIC, CNA, HBA FC)
- Configurer l'initiateur (pour iSCSI et FCoE) et les paramètres de la cible de stockage (pour iSCSI, FCoE et FC)
- Spécifiez la persistance ou l'effacement des valeurs configurées sur une perte d'alimentation CA du système et des réinitialisations à froid et à chaud du système.

Les valeurs configurées pour les adresses virtuelles, l'initiateur et les cibles de stockage peuvent varier en fonction de la gestion de l'alimentation principale au cours de la réinitialisation du système et selon que la carte NIC, le CNA ou le HBA FC dispose ou non d'une alimentation auxiliaire. La persistance des paramètres de l'identité d'E/S peut être obtenue en fonction de la configuration de la stratégie effectuée à l'aide de l'iDRAC.

Les stratégies de persistance ne s'appliquent que si la fonctionnalité d'identité d'E/S est activée. Chaque fois que le système est réinitialisé ou mis sous tension, les valeurs sont conservées ou effacées en fonction des paramètres de la stratégie.

REMARQUE : Une fois les valeurs effacées, vous ne pouvez pas les ré-appliquer avant d'exécuter la tâche de configuration.

Prise en charge de l'optimisation des identités d'E/S dans l'interface Web

Dans les **Propriétés du port** de la carte NIC spécifique (**Périphériques réseau** > **du système**), si l'option **Fonctionnalité de stratégie de persistance** affiche **Compatible** pour la carte NIC spécifique, la carte prend en charge l'optimisation d'identité d'E/S.

Comportement de l'adresse virtuelle/attribuée à distance et de la stratégie de persistance lorsque le contrôleur iDRAC est défini sur le mode Console ou Adresse attribuée à distance

Le tableau suivant décrit la configuration de la gestion des adresses virtuelles (VAM) et le comportement de la stratégie de persistance, et les dépendances.

Tableau 36. Comportement de l'adresse virtuelle/attribuée à distance et de la stratégie de persistance

État de la fonction d'adresse attribuée à distance dans OME Modular	Mode défini dans la configuration iDRAC	État de la fonction d'identité d'E/S dans l'iDRAC	SCP	Stratégie de persistance	Effacer la stratégie de persistance : adresse virtuelle
Adresse attribuée à distance activée	Mode Adresse attribuée à distance	Activé	Gestion des adresses virtuelles (VAM) configurée	VAM configuré persiste	Défini sur Adresse attribuée à distance
Adresse attribuée à distance activée	Mode Adresse attribuée à distance	Activé	VAM non configuré	Défini sur Adresse attribuée à distance	Pas de persistance : défini sur Adresse attribuée à distance
Adresse attribuée à distance activée	Mode Adresse attribuée à distance	Désactivé	Configuré à l'aide du chemin défini dans le Lifecycle Controller	Défini sur Adresse attribuée à distance pour ce cycle	Pas de persistance : défini sur Adresse attribuée à distance
Adresse attribuée à distance activée	Mode Adresse attribuée à distance	Désactivé	VAM non configuré	Défini sur Adresse attribuée à distance	Défini sur Adresse attribuée à distance
Adresse attribuée à distance désactivée	Mode Adresse attribuée à distance	Activé	VAM configuré	VAM configuré persiste	Persistance uniquement : l'effacement n'est pas possible
Adresse attribuée à distance désactivée	Mode Adresse attribuée à distance	Activé	VAM non configuré	Définir sur l'adresse MAC du matériel	Aucune prise en charge de la persistance. Dépend du comportement de la carte
Adresse attribuée à distance désactivée	Mode Adresse attribuée à distance	Désactivé	Configuré à l'aide du chemin défini dans le Lifecycle Controller	La configuration du Lifecycle Controller persiste pour ce cycle	Aucune prise en charge de la persistance. Dépend du comportement de la carte
Adresse attribuée à distance désactivée	Mode Adresse attribuée à distance	Désactivé	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel
Adresse attribuée à distance activée	Mode Console	Activé	VAM configuré	VAM configuré persiste	Tant la persistance que l'effacement doivent fonctionner

Tableau 36. Comportement de l'adresse virtuelle/attribuée à distance et de la stratégie de persistance (suite)

État de la fonction d'adresse attribuée à distance dans OME Modular	Mode défini dans la configuration iDRAC	État de la fonction d'identité d'E/S dans l'iDRAC	SCP	Stratégie de persistance	Effacer la stratégie de persistance : adresse virtuelle
Adresse attribuée à distance activée	Mode Console	Activé	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel
Adresse attribuée à distance activée	Mode Console	Désactivé	Configuré à l'aide du chemin défini dans le Lifecycle Controller	La configuration du Lifecycle Controller persiste pour ce cycle	Aucune prise en charge de la persistance. Dépend du comportement de la carte
Adresse attribuée à distance désactivée	Mode Console	Activé	VAM configuré	VAM configuré persiste	Tant la persistance que l'effacement doivent fonctionner
Adresse attribuée à distance désactivée	Mode Console	Activé	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel
Adresse attribuée à distance désactivée	Mode Console	Désactivé	Configuré à l'aide du chemin défini dans le Lifecycle Controller	La configuration du Lifecycle Controller persiste pour ce cycle	Aucune prise en charge de la persistance. Dépend du comportement de la carte
Adresse attribuée à distance activée	Mode Console	Désactivé	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel

REMARQUE :

- La configuration du remplacement de pièces pour les cartes prenant en charge les partitions fonctionne correctement lorsque l'attribut VirtualizationMode (permettant d'activer le nombre de partitions) est identique à celui de la carte remplacée et de la carte NIC présente sur le serveur.
- La configuration du remplacement de pièces ne se déclenche pas lorsque l'attribut VirtualizationMode (nombre de partitions) de la carte remplacée ne correspond pas à celui de la carte NIC présente sur le serveur.
- Pendant la fenêtre de remplacement de pièces avant CSIOR, le Lifecycle Controller restaure la configuration de la carte NIC. Cela implique un démarrage à froid suivi d'un démarrage à chaud. Après les deux redémarrages, la carte NIC dispose du même firmware qui est installé lors du processus de restauration.
- La stratégie de persistance s'applique à chaque redémarrage en fonction de la règle. Ici, lors du démarrage à froid, les identités virtuelles ne sont pas appliquées en raison d'une non-correspondance de version du firmware et de la suppression des données de persistance.
- La fonctionnalité de stratégie de persistance vérifie les ID de PCI et la version de firmware de la carte NIC actuelle et précédente du même fournisseur qui est remplacée. En cas d'absence de correspondance de ces champs, les identités virtuelles ne sont pas appliquées et les données de persistance (identités virtuelles) sont également supprimées de l'iDRAC.
- Pour le remplacement de pièces, le fournisseur doit conserver les mêmes ID de PCI et la même version de firmware ou vous devez exécuter le déploiement de la tâche/du modèle VAM.

Comportement du système pour Adresse Flex et l'identité d'E/S

Tableau 37. Comportement du système pour FlexAddress et l'identité d'E/S

Type	État de la fonction FlexAddress dans le CMC	État de la fonction d'identité d'E/S dans l'iDRAC	Disponibilité de VA d'agent à distance pour le cycle de redémarrage	Source de programmation VA	Comportement de persistance de VA de cycle de redémarrage
Serveur avec une persistance équivalente à FA	Activé	Désactivé	S/O	FlexAddress depuis CMC	Spécification par FlexAddress

Tableau 37. Comportement du système pour FlexAddress et l'identité d'E/S (suite)

Type	État de la fonction FlexAddress dans le CMC	État de la fonction d'identité d'E/S dans l'iDRAC	Disponibilité de VA d'agent à distance pour le cycle de redémarrage	Source de programmation VA	Comportement de persistance de VA de cycle de redémarrage
	Non Applicable (N/A), activé ou désactivé	Activé	Oui : Nouveau ou persistant	Adresse virtuelle de l'agent distant	Spécification par FlexAddress
			Non	Adresse virtuelle effacée	
	Désactivé	Désactivé	S/O	S/O	S/O
Serveur avec fonction de stratégie de persistance VAM	Activé	Désactivé	S/O	FlexAddress depuis CMC	Spécification par FlexAddress
	Activé	Activé	Oui : Nouveau ou persistant	Adresse virtuelle de l'agent distant	Paramètre de stratégie par l'agent à distance
			Non	FlexAddress depuis CMC	Spécification par FlexAddress
	Désactivé	Activé	Oui : Nouveau ou persistant	Adresse virtuelle de l'agent distant	Paramètre de stratégie par l'agent à distance
			Non	Adresse virtuelle effacée	
	Désactivé	Désactivé	S/O	S/O	S/O

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 de l'appareil survient lors du démarrage unique du système et est optimisée pour les performances du temps de démarrage.

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, iDRAC et les cartes réseau sont mis à jour vers la version la plus récente du micrologiciel.

Après l'activation de la fonction d'optimisation d'identité d'E/S, exportez le fichier de profil de configuration du serveur à partir d'iDRAC, modifiez les attributs d'identité d'E/S requis dans le fichier SCP et réimportez le fichier sur iDRAC.

REMARQUE : Les attributs d'identité d'E/S ne doivent être définis qu'à l'aide du protocole SCP pour les rendre persistants lors des redémarrages. L'utilisation d'autres méthodes pour les définir ne permet pas de les rendre persistants.

Pour obtenir la liste des attributs d'optimisation d'identité d'E/S que vous pouvez modifier dans le fichier SCP, voir le document **Profil de carte NIC** disponible sur Page de support Dell.

REMARQUE : Ne modifiez pas les attributs autres que ceux d'optimisation d'identité d'E/S.

Activation ou désactivation de l'optimisation d'identité des E/S via l'interface Web

Pour activer ou désactiver l'optimisation d'identité d'E/S :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Optimisation d'identité d'E/S**.
   La page **Optimisation d'identité des E/S** s'affiche.
2. Cliquez sur l'onglet **Optimisation d'identité des E/S**, puis sélectionnez l'option **Activer** pour activer cette fonctionnalité. Pour le 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 Enabled
```

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 Disabled
```

Pour afficher le réglage de l'optimisation d'identité d'E/S, utilisez la commande :

```
racadm get iDRAC.IOIDOpt
```

Seuil d'usure du disque SSD

iDRAC vous offre la possibilité de configurer les seuils d'endurance d'écriture nominale restante pour tous les disques SSD et les valeurs de secours disponibles des disques SSD PCIe NVMe.

Lorsque la durée d'endurance d'écriture nominale restante des disques SSD et les valeurs de secours des disques SSD PCIe NVMe sont inférieures au seuil, alors l'iDRAC enregistre cet évènement dans le journal LC et en fonction du type d'alerte sélectionné, iDRAC permet également de réaliser une alerte e-mail, une interruption SNMP, une alerte IPMI, une connexion à un journal Syslog distant, les évènements WS et la connexion au système d'exploitation.

iDRAC alerte l'utilisateur lorsque l'endurance d'écriture nominale restante du disque SSD passe en dessous du seuil défini, de sorte que l'administrateur système peut réaliser une sauvegarde du disque SSD ou le remplacer.

Pour les disques SSD PCIe NVMe uniquement, iDRAC affiche la **valeur de secours disponible** et fournit un seuil d'avertissement. La **valeur de secours disponible** ne l'est pas pour les disques SSD qui sont connectés derrière PERC et HBA.

Configuration des fonctionnalités d'alerte de seuil d'usure du disque SSD à l'aide de l'interface Web

Pour configurer l'endurance d'écriture nominale restante et les seuils d'alerte de secours disponibles à l'aide de l'interface Web :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Seuils d'usure du disque SSD**.
   La page **Seuils d'usure du disque SSD** s'affiche.
2. **Endurance d'écriture nominale restante** : vous pouvez définir une valeur comprise entre 1 et 99 %. La valeur par défaut est 10 %. Le type d'alerte pour cette fonctionnalité est le message d'**Endurance d'écriture nominale restante SSD** et l'alerte de sécurité est le message d'**Avertissement** à la suite d'un événement de seuil.
3. **Seuil d'alerte de secours disponible** : vous pouvez définir une valeur comprise entre 1 et 99 %. La valeur par défaut est 10 %. Le type d'alerte pour cette fonctionnalité est le message d'**Endurance d'écriture nominale restante SSD** et l'alerte de sécurité est le message d'**Avertissement** à la suite d'un événement de seuil.

Configuration des fonctionnalités d'alerte de seuil d'usure des disques SSD à l'aide de RACADM

Pour configurer l'endurance d'écriture nominale restante, utilisez la commande :

```
racadm set System.Storage.RemainingRatedWriteEnduranceAlertThreshold n
```

, où n = 1 à 99 %

Pour configurer le seuil d'alerte de valeur de secours disponible, utilisez la commande :

```
racadm System.Storage.AvailableSpareAlertThreshold n
```

, où n = 1 à 99 %

Configuration des paramètres de la stratégie de persistance

À l'aide de l'identité d'E/S, vous pouvez configurer des stratégies indiquant les comportements de réinitialisation du système et de cycle de marche/arrêt qui déterminent la persistance ou l'effacement des paramètres de l'adresse virtuelle, de l'initiateur et des cibles de stockage. Chaque attribut de stratégie de persistance individuelle s'applique à tous les ports et les partitions de tous les périphériques appropriés du système. Le comportement des périphériques varie : ils peuvent être alimentés par une unité auxiliaire ou non.

REMARQUE : La fonctionnalité de **Politique de persistance** peut ne pas fonctionner lorsqu'elle est définie sur la valeur par défaut. Si l'attribut **VirtualAddressManagement** est défini sur **FlexAddress** sur l'iDRAC, assurez-vous de définir l'attribut **VirtualAddressManagement** sur le mode **Console** dans l'iDRAC.

Vous pouvez configurer les stratégies de persistance suivantes :

- Adresse virtuelle : périphériques alimentés par auxiliaire
- Adresse virtuelle : périphériques qui ne sont alimentés par auxiliaire
- Initiateur
- Cible de stockage

Avant d'appliquer la stratégie de persistance, vérifiez les points suivants :

- Faites l'inventaire du matériel réseau au moins une fois, c'est-à-dire activez la Collecte de l'inventaire du système au redémarrage.
- Activer l'optimisation d'identité d'E/S

Les événements sont journalisés dans le journal du Lifecycle Controller dans les cas suivants :

- L'optimisation de l'identité d'E/S est activée ou désactivée.
- La stratégie de persistance est modifiée.
- L'adresse virtuelle, l'initiateur et les valeurs cibles sont définis selon la stratégie. Une seule entrée de journal est enregistrée pour les périphériques configurés et les valeurs qui sont définies pour ces périphériques lors de l'application de la stratégie.

Des actions d'événements sont activées en cas de notifications SNMP ou par email. Les journaux sont également inclus dans le syslog distant.

Valeurs par défaut de la stratégie de persistance

Tableau 38. Valeurs par défaut de la stratégie de persistance

Stratégie de persistance	Perte d'alimentation CA	Démarrage à froid	Démarrage à chaud
Adresse virtuelle : périphériques à alimentation auxiliaire	Non sélectionné	Sélectionné	Sélectionné
Adresse virtuelle : périphériques à alimentation non auxiliaire	Non sélectionné	Non sélectionné	Sélectionné
Initiateur	Sélectionné	Sélectionné	Sélectionné
Cible de stockage	Sélectionné	Sélectionné	Sélectionné

REMARQUE : Lorsqu'une stratégie persistante est désactivée, et lorsque vous effectuez l'action de perte de l'adresse virtuelle, la réactivation de la stratégie persistante ne récupère pas l'adresse virtuelle. Vous devez définir l'adresse virtuelle à nouveau après avoir activé la stratégie persistante.

REMARQUE : Si une stratégie de persistance est en vigueur et que les adresses virtuelles, l'initiateur ou les cibles de stockage sont définis sur une partition de périphérique CNA, ne réinitialisez pas ou n'effacez pas les valeurs configurées pour les adresses virtuelles, l'initiateur et les cibles de stockage avant de modifier l'attribut VirtualizationMode ou la personnalité de la partition. L'action

est effectuée automatiquement lorsque vous désactivez la stratégie de persistance. Vous pouvez également utiliser une tâche de configuration afin de définir explicitement les attributs d'adresse virtuelle sur 0s et les valeurs de l'initiateur et des cibles de stockage telles que définies dans Valeurs par défaut des cibles de stockage et de l'initiateur iSCSI.

Configuration des paramètres de la règle de persistance à l'aide de l'interface Web iDRAC

Pour configurer la règle de persistance :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **Optimisation d'identité d'E/S**.
2. Cliquez sur l'onglet **Optimisation d'identité d'E/S**.
3. Dans la section **Règle de persistance**, sélectionnez une ou plusieurs des actions suivantes pour chaque règle de persistance :
   - **Redémarrage à chaud** : les paramètres d'adresse virtuelle ou de cible sont conservés en cas de redémarrage à chaud.
   - **Redémarrage à froid** : les paramètres d'adresse virtuelle ou de cible sont conservés en cas de redémarrage à froid.
   - **Perte d'alimentation CA** : les paramètres d'adresse virtuelle ou de cible sont conservés en cas de perte d'alimentation CA.
4. Cliquez sur **Appliquer**.
   Les règles de persistance sont configurées.

Configuration des paramètres de la règle de persistance à l'aide de RACADM

Pour définir la règle de persistance, utilisez l'objet racadm suivant avec la sous-commande **set** :

- Pour les adresses virtuelles, utilisez les objets **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** et **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd**
- Pour l'initiateur, utilisez l'objet **iDRAC.IOIDOPT.InitiatorPersistencePolicy**
- Pour les cibles de stockage, utilisez l'objet **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**

Valeurs par défaut des cibles de stockage et de l'initiateur iSCSI

Les tableaux ci-dessous fournissent la liste des valeurs par défaut de l'initiateur iSCSI et des cibles de stockage lorsque les règles de persistance sont effacées.

Tableau 39. Valeurs par défaut de l'initiateur iSCSI

Initiateur iSCSI	Valeurs par défaut en mode IPv4	Valeurs par défaut en mode IPv6
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::

Tableau 39. Valeurs par défaut de l'initiateur iSCSI (suite)

Initiateur iSCSI	Valeurs par défaut en mode IPv4	Valeurs par défaut en mode IPv6
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
iscsiInitiatorName	Valeur effacée	Valeur effacée
IscsiInitiatorChapId	Valeur effacée	Valeur effacée
IscsiInitiatorChapPwd	Valeur effacée	Valeur effacée
IPVer	Ipv4	Par Ipv6

Tableau 40. Valeurs par défaut des attributs de cibles de stockage ISCSI

Attributs de cibles de stockage iSCSI	Valeurs par défaut en mode IPv4	Valeurs par défaut en mode IPv6
ConnectFirstTgt	Désactivé	Désactivé
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	Valeur effacée	Valeur effacée
FirstTgtChapId	Valeur effacée	Valeur effacée
FirstTgtChapPwd	Valeur effacée	Valeur effacée
FirstTgtIpVer	Ipv4	S/O
ConnectSecondTgt	Désactivé	Désactivé
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	Valeur effacée	Valeur effacée
SecondTgtChapId	Valeur effacée	Valeur effacée
SecondTgtChapPwd	Valeur effacée	Valeur effacée
SecondTgtIpVer	Ipv4	S/O

19

Gestion de périphériques de stockage

L'iDRAC prend en charge les contrôleurs PERC 12 et BOSS N1.

REMARQUE : L'effacement des caches matériels échoue sur un contrôleur PERC12 externe configuré. Exécutez l'opération de réinitialisation de la configuration avant d'effacer le cache matériel.

REMARQUE :

- Les contrôleurs BOSS ne prennent en charge que RAID 0 et RAID 1.
- Tous les disques virtuels étrangers détectés derrière les contrôleurs BOSS doivent être effacés du BIOS HII ou à l'aide de l'opération de réinitialisation du contrôleur.
- Pour les contrôleurs BOSS, il est possible que l'ensemble des informations relatives aux disques virtuels ne soient pas disponibles lorsque les deux disques physiques sont déconnectés et reconnectés.
- Pour toute mise à jour nécessitant une réinitialisation/un redémarrage de l'iDRAC ou si l'iDRAC est redémarré, il est recommandé de vérifier si l'iDRAC est prêt en attendant quelques secondes, avec un délai d'expiration maximum de 5 minutes, avant d'utiliser une autre commande.
- Pour les contrôleurs PERC12, l'extension de capacité en ligne (OCE) avec ajout de disque est uniquement possible sur un disque virtuel de taille complète. L'OCE avec ajout de disque n'est pas exécutée sur les disques virtuels répartis.
- Pour éviter toute erreur imprévisible, il est recommandé de ne pas effectuer d'opération liée au stockage lorsqu'une tâche de stockage est en cours.

iDRAC a étendu sa gestion sans agent pour inclure la configuration directe des contrôleurs PERC. Vous pouvez ainsi configurer à distance les composants de stockage connectés à votre système au moment de l'exécution. Ces composants incluent les contrôleurs RAID et non RAID ainsi que les canaux, ports, boîtiers et disques qui leur sont associés.

L'intégralité des opérations de détection, de topologie, de surveillance d'intégrité et de configuration du sous-système de stockage sont réalisées dans le cadre de l'infrastructure CEM (Comprehensive Embedded Management) en communiquant avec les contrôleurs PERC internes et externes via l'interface I2C et le protocole MCTP.

REMARQUE : Le RAID logiciel (SWRAID) n'est pas compatible avec l'infrastructure CEM et n'est donc pas pris en charge dans l'interface utilisateur de l'iDRAC. SWRAID peut être géré à l'aide de RACADM ou de Redfish.

Avec le contrôleur iDRAC, vous pouvez effectuer la plupart des fonctionnalités disponibles avec OpenManage Storage Management, notamment les commandes de configuration en temps réel (Sans redémarrage) (par exemple, création d'un disque virtuel). Vous pouvez configurer intégralement un système RAID avant d'installer le système d'exploitation.

Vous pouvez configurer et gérer les fonctionnalités du contrôleur sans accéder au BIOS. Ces fonctionnalités incluent la configuration des disques virtuels et l'application des niveaux RAID et des disques de secours dans le cadre de la protection des données. Vous pouvez également exécuter d'autres fonctionnalités du contrôleur telles que la reconstruction et le dépannage. Vous pouvez protéger vos données en configurant leur redondance ou en affectant des disques de secours.

REMARQUE : Si le paramètre BIOS Volume Management Device (VMD) (avec prise en charge du module ID) est activé sur un serveur PowerEdge, évitez de configurer des disques NVMe rattachés au processeur pour éviter tout comportement imprévisible.

Les périphériques de stockage sont les suivants :

- Contrôleur : la plupart des systèmes d'exploitation ne lisent ni n'écrivent directement de données sur les disques ; ils envoient plutôt des instructions de lecture et d'écriture à un contrôleur. Le contrôleur s'inscrit comme le matériel de votre système qui interagit directement avec les disques afin d'écrire et de récupérer des données. Un contrôleur dispose de connecteurs (canaux ou ports) raccordés à un ou plusieurs disques physiques ou à un boîtier contenant des disques physiques. Les contrôleurs RAID peuvent étendre les limites des disques pour augmenter la quantité d'espace de stockage, ou créer un disque virtuel, en utilisant la capacité de plusieurs disques. Les contrôleurs effectuent également d'autres tâches, telles que le lancement de reconstructions ou l'initialisation de disques. Pour réaliser leurs tâches, les contrôleurs nécessitent des logiciels spécifiques appelés firmwares et pilotes. Pour fonctionner correctement, le contrôleur doit disposer du firmware et des pilotes installés à la version minimale requise. Les différents contrôleurs lisent les données, les écrivent et exécutent leurs tâches différemment. Il est recommandé de connaître ces fonctionnalités pour gérer votre stockage le plus efficacement possible.
- Les disques ou appareils physiques résident dans un boîtier ou sont rattachés au contrôleur. Sur un contrôleur RAID, les disques ou périphériques physiques permettent de créer des disques virtuels.

- Disque virtuel : il s'agit du stockage créé par un contrôleur RAID à partir d'un ou plusieurs disques physiques. Bien qu'un disque virtuel puisse être créé à partir de plusieurs disques physiques, il est considéré par le système d'exploitation comme un disque unique. En fonction du niveau RAID utilisé, le disque virtuel peut conserver les données redondantes en cas de panne de disque ou offrir des attributs de performances spécifiques. Les disques virtuels ne peuvent être créés que sur un contrôleur RAID.
- Boîtier : il est relié au système en externe tandis que le fond de panier et ses disques physiques sont internes. Si les boîtiers sont connectés en configuration multipath, assurez-vous que les combinaisons de ports suivantes sont utilisées pour la connexion aux contrôleurs :
  - Port 0 et port 2
  - Port 1 et port 3
- Fond de panier : il est similaire à un boîtier. Dans un fond de panier, le connecteur du contrôleur et les disques physiques sont reliés au boîtier. Cependant, le fond de panier n'offre pas les fonctionnalités de gestion (capteurs de température, alarmes, etc.) associées aux boîtiers externes. Les disques physiques peuvent être intégrés à un boîtier ou connectés au fond de panier du système.

REMARQUE : L'inventaire de la configuration maximale avec 192 disques physiques environ peut durer 30 minutes minimum.

REMARQUE : Lorsqu'un système dispose d'une grande matrice de composants de stockage, comme 240 disques virtuels et 60 disques, certaines opérations de stockage en attente ou opérations d'abandon en attente peuvent rencontrer des échecs accompagnés de l'erreur RAC0508.

REMARQUE : Lorsqu'un ou plusieurs fonds de panier sont connectés à un module d'extension, la position du boîtier s'affiche comme **Inconnu**.

REMARQUE : Sur certaines plateformes, l'insertion/le retrait à chaud du module tiroir extractible n'est pas pris en charge et vous pouvez voir des erreurs inattendues. Celui-ci doit être mis hors tension avant l'insertion/le retrait à chaud.

Outre la gestion des disques physiques intégrés à un boîtier, vous pouvez surveiller l'état des ventilateurs, des blocs d'alimentation et des capteurs de température du boîtier. Les boîtiers sont enfichables à chaud. La connexion à chaud représente l'ajout d'un composant à un système alors que le système d'exploitation est exécuté.

REMARQUE : L'état des disques qui sont retirés à chaud est défini sur **Retiré**, et les informations sur les disques sont disponibles dans les inventaires du matériel et du firmware jusqu'au prochain redémarrage de l'hôte.

Les périphériques physiques connectés au contrôleur doivent disposer du firmware le plus récent. Pour connaître les derniers firmwares pris en charge, contactez votre prestataire de services.

REMARQUE : Si vous exécutez la mise à jour du firmware sur des disques enfichables à chaud, le journal PR36 peut être absent des journaux Lifecycle, même si la mise à jour a réussi. Pour éviter cela, exécutez un redémarrage de l'hôte avant la mise à jour du firmware.

REMARQUE : PR36 n'est pas enregistré pour les batteries de secours (BBU) et les unités de traitement des données (DPU) après les mises à jour du firmware.

Les événements de stockage du contrôleur PERC sont adressés comme interruptions SNMP, le cas échéant. Toutes les modifications apportées aux configurations de stockage sont journalisées dans le journal Lifecycle.

REMARQUE : Après avoir exécuté un redémarrage à chaud du serveur, l'iDRAC peut signaler un journal Lifecycle PDR8 pour les disques connectés derrière les contrôleurs PERC.

REMARQUE : Dans l'iDRAC, vous pouvez voir le fond de panier/boîtier associé au contrôleur PERC de vos systèmes. Ce boîtier montre 16 logements (même si votre système ne prend pas en charge autant de disques).

Dans les systèmes où les disques sont connectés directement au contrôleur RAID, une entrée est créée pour chaque connexion de disque possible au contrôleur PERC. Le contrôleur PERC prend en charge jusqu'à 16 disques connectés par câble, c'est la raison pour laquelle 16 logements sont signalés.

Tableau 41. Fonctionnalité PERC

Fonctionnalité PERC	Contrôleur prenant en charge la configuration CEM
En temps réel	Si des tâches sont en attente ou planifiées pour un contrôleur, elles doivent être effacées. Sinon, vous devez attendre qu'elles se terminent avant d'appliquer la configuration au moment de l'exécution. Un redémarrage n'est pas obligatoire pour les tâches en temps réel ou au moment de l'exécution.
Simulé	S/O

Sujets :

Présentation des concepts RAID

Storage Management utilise la technologie RAID (Redundant Array of Independent Disks) pour fournir des fonctions de gestion de stockage. Pour comprendre Storage Management vous devez avoir une bonne connaissance des concepts RAID et de la façon dont les contrôleurs RAID et le système d'exploitation détectent l'espace disque sur votre système.

Qu'est-ce que l'application RAID

RAID est une technologie qui permet de gérer le stockage des données sur les disques physiques qui résident sur le système ou sont associés au système. Cette technologie permet de répartir les disques physiques, afin que la capacité de stockage combinée de plusieurs disques physiques puisse être traitée comme un seul espace disque étendu. Un autre aspect clé de la technologie RAID est la possibilité de conserver des données redondantes, qui peuvent être utilisées pour restaurer les données en cas de panne de disque. RAID utilise différentes techniques, telles que l'agrégation par bandes, la mise en miroir et la parité, pour stocker et reconstruire les données. Il existe différents niveaux de RAID qui font appel à diverses méthodes pour stocker et reconstruire les données. Les niveaux de RAID ont des caractéristiques distinctes en termes de performances de lecture/écriture, de protection des données et de capacité de stockage. Tous les niveaux de RAID ne conservent pas les données redondantes, ce qui signifie que pour certains niveaux de RAID, les données perdues ne peuvent pas être restaurées. Le niveau de RAID que vous choisissez dépend de ce que vous souhaitez prioriser : les performances, la protection ou la capacité de stockage.

REMARQUE : Le RAID Advisory Board (RAB) définit les spécifications utilisées pour implémenter la technologie RAID. Bien que le RAB définisse les niveaux de RAID, l'implémentation commerciale des niveaux de RAID par divers fournisseurs peut différer des spécifications RAID réelles. Une implémentation d'un fournisseur particulier peut affecter les performances de lecture et d'écriture, ainsi que le degré de redondance des données.

RAID matériel et logiciel

La technologie RAID peut être implémentée avec du matériel ou des logiciels. Un système utilisant un RAID matériel dispose d'un contrôleur RAID qui implémente les niveaux RAID et traite les lectures et écritures de données sur les disques physiques. Lors de l'utilisation d'un RAID logiciel fourni par le système d'exploitation, le système d'exploitation implémente les niveaux de RAID. C'est la raison pour laquelle l'utilisation d'un RAID logiciel peut ralentir les performances du système. Vous pouvez en revanche utiliser un RAID logiciel et des volumes RAID matériels pour offrir de meilleures performances et une plus grande diversité dans la configuration des volumes RAID. Par exemple, vous pouvez mettre en miroir une paire de volumes RAID 5 matériels sur deux contrôleurs RAID pour assurer la redondance du contrôleur RAID.

Concepts de RAID

RAID utilise des techniques particulières pour écrire des données sur les disques. Ces techniques permettent à RAID de fournir une redondance des données ou de meilleures performances. Ces techniques sont les suivantes :

- Mise en miroir : duplication des données d'un disque physique vers un autre disque physique. La mise en miroir assure la redondance des données en conservant deux copies des mêmes données sur des disques physiques différents. Si l'un des disques du miroir tombe en panne, le système peut continuer à fonctionner grâce au disque non touché. Les deux côtés du miroir contiennent toujours les mêmes données. Chaque côté du miroir peut agir en tant que côté opérationnel. Un groupe de disques RAID en miroir est comparable en termes de performances à un groupe de disques RAID 5 dans les opérations de lecture, mais plus rapide dans les opérations d'écriture.
- Agrégation par bandes : l'agrégation par bandes des disques écrit les données sur tous les disques physiques d'un disque virtuel. Chaque bande de répartition correspond à une plage d'adresses de données sur le disque virtuel. Ces adresses sont associées par adressage séquentiel (sous forme d'unités de taille fixe) à chaque disque physique membre du disque virtuel. Par exemple, si le disque virtuel comprend cinq disques physiques, la bande de répartition écrit des données sur les disques physiques un à cinq sans aucune répétition sur deux disques. La quantité d'espace occupée par une bande est la même sur chaque disque physique. La portion des données réparties qui réside sur un disque physique est un élément de bande. L'agrégation par bandes en elle-même ne fournit aucune redondance des données, sauf si elle est associée à un mécanisme de parité.
- Taille de répartition : l'espace disque total consommé par une répartition, sans compter un disque de parité. Prenons l'exemple d'une répartition dont l'espace disque est de 64 Ko et dans laquelle 16 Ko de données résident sur chaque disque de la répartition. Dans ce cas, la taille de répartition est de 64 Ko et la taille de l'élément de répartition est de 16 Ko.
- Segment de bande : un segment de bande est la partie d'une bande qui réside sur un seul disque physique.
- Taille de l'élément de répartition : quantité d'espace disque consommée par un élément de répartition. Prenons l'exemple d'une répartition dont l'espace disque est de 64 Ko et dans laquelle 16 Ko de données résident sur chaque disque de la répartition. Dans ce cas, la taille de l'élément de répartition est de 16 Ko et la taille de répartition est de 64 Ko.
- Parité : la parité fait référence aux données redondantes qui sont conservées à l'aide d'un algorithme en combinaison avec l'agrégation par bandes. Lorsque l'un des disques répartis tombe en panne, les données peuvent être reconstruites à partir des informations de parité à l'aide de l'algorithme.
- Répartition : une répartition est une technique RAID utilisée pour combiner l'espace de stockage de groupes de disques physiques dans un disque virtuel RAID 10, 50 ou 60.

Niveaux RAID

Chaque niveau de RAID utilise une combinaison spécifique de mise en miroir, d'agrégation par bandes et de parité pour fournir la redondance des données ou améliorer les performances de lecture et d'écriture. Pour obtenir des informations spécifiques sur chaque niveau de RAID, voir Sélection des niveaux de RAID.

Organisation du stockage de données à des fins de disponibilité et de performances

RAID fournit différentes méthodes ou niveaux de RAID pour organiser le stockage sur disque. Certains niveaux de RAID conservent des données redondantes afin que vous puissiez restaurer les données après une panne de disque. Les différents niveaux de RAID impliquent également une augmentation ou une diminution des performances d'E/S (lecture et écriture) d'un système.

La maintenance des données redondantes nécessite l'utilisation de disques physiques supplémentaires. La possibilité d'une panne de disque augmente lorsque le nombre de disques augmente. En raison des différences de performances d'E/S et de redondance, un niveau de RAID peut être plus approprié qu'un autre en fonction des applications de l'environnement d'exploitation et de la nature des données stockées.

Lorsque vous choisissez un niveau de RAID, vous pouvez vous attendre aux performances et aux éléments à prendre en compte en matière de coût suivants :

- **Disponibilité ou tolérance de panne** : la disponibilité ou la tolérance de panne désigne la capacité d'un système à maintenir les opérations et à fournir un accès aux données, même lorsque l'un de ses composants est défaillant. Dans les volumes RAID, la disponibilité ou la tolérance aux pannes est assurée par la conservation des données redondantes. Les données redondantes incluent des miroirs (données dupliquées) et des informations de parité (reconstruction des données à l'aide d'un algorithme).
- **Performances** : les performances de lecture et d'écriture peuvent augmenter ou diminuer en fonction du niveau de RAID que vous choisissez. Certains niveaux de RAID peuvent être plus appropriés pour des applications particulières.
- **Rentabilité** : la conservation des données redondantes ou des informations de parité associées aux volumes RAID nécessite de l'espace disque supplémentaire. Dans les situations où les données sont temporaires, faciles à reproduire ou non essentielles, le coût supplémentaire lié à la redondance des données peut ne pas être justifié.

- **Temps moyen entre les pannes (MTBF)** : l'utilisation de disques supplémentaires pour assurer la redondance des données augmente également le risque de panne de disque à un moment donné. Bien que cette option ne puisse pas être évitée dans les situations où les données redondantes sont une exigence, elle a des implications sur la charge applicative des équipes de support système au sein de votre organisation.
- **Volume** : le volume désigne un seul disque virtuel non RAID. Vous pouvez créer des volumes à l'aide d'utilitaires externes tels que O-ROM <Ctrl> <r>. Storage Management ne prend pas en charge la création de volumes. Toutefois, vous pouvez afficher les volumes et utiliser les disques de ces volumes pour la création de nouveaux disques virtuels ou l'extension de capacité en ligne (OCE) des disques virtuels existants, à condition que de l'espace libre soit disponible.

Choix des niveaux de RAID

Vous pouvez utiliser le RAID pour contrôler le stockage de données sur plusieurs disques. Chaque niveau de RAID ou concaténation a différentes caractéristiques de performances et de protection des données.

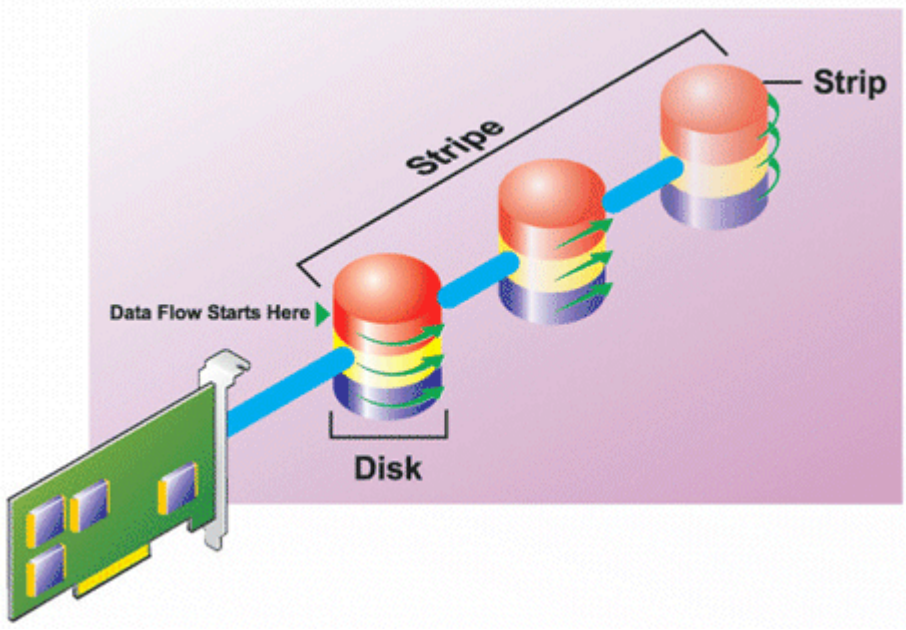
REMARQUE : Les contrôleurs PERC H3xx ne prennent pas en charge les niveaux RAID 6 et 60.

Les rubriques suivantes fournissent des informations sur la façon dont chaque niveau de RAID stocke les données ainsi que leurs caractéristiques de performances et de protection des données :

- Niveau de RAID 0 (agrégation par bandes)
- Niveau de RAID 1 (mise en miroir)
- Niveau de RAID 5 (agrégation par bandes avec parité distribuée)
- Niveau de RAID 6 (agrégation par bandes avec parité distribuée supplémentaire)
- Niveau de RAID 50 (agrégation par bandes sur des ensembles RAID 5)
- Niveau de RAID 60 (agrégation par bandes sur des ensembles RAID 6)
- Niveau de RAID 10 (agrégation par bandes sur des ensembles miroir)

Niveau de RAID 0 - Agrégation par bandes

RAID 0 utilise l'agrégation par bandes des données, ce qui entraîne l'écriture des données de segments de même taille sur les disques physiques. RAID 0 ne fournit pas de redondance des données.

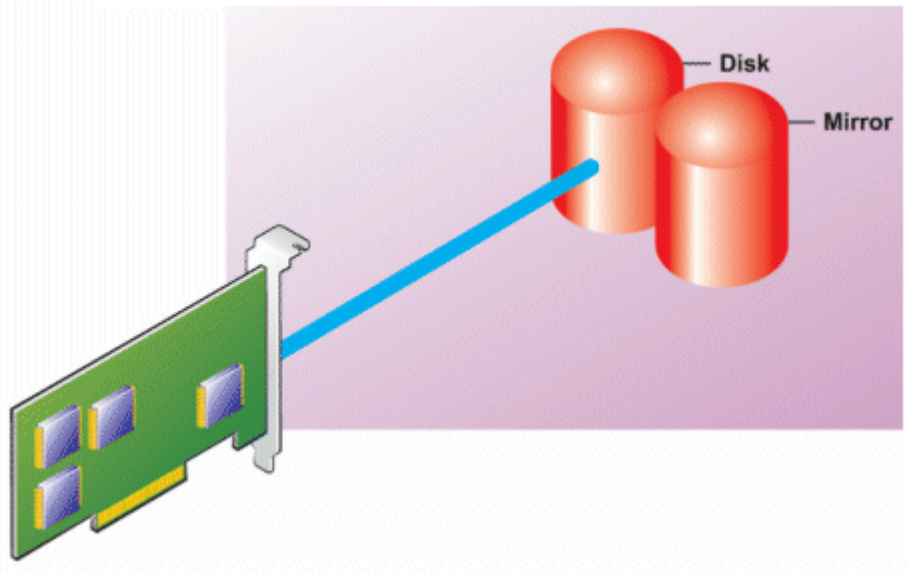


RAID 0

- Disques des groupes **n** comme disque virtuel important doté d'une capacité de (taille de disque la plus petite) *__n__ disques.
- Les données sont stockées sur les disques de manières alternative.
- Aucune donnée redondante n'est conservée. Lorsqu'un disque échoue, le disque virtuel important échoue sans pouvoir reconstruire les données de quelque façon que ce soit.
- Les performances de lecture-écriture sont meilleures.

Niveau de RAID 1 - mise en miroir

RAID 1 est la forme la plus simple de maintenance des données redondantes. Dans RAID 1, les données sont en miroir ou dupliquées sur un ou plusieurs disques physiques. Si un disque physique tombe en panne, vous pouvez reconstruire les données à l'aide des données de l'autre côté du miroir.

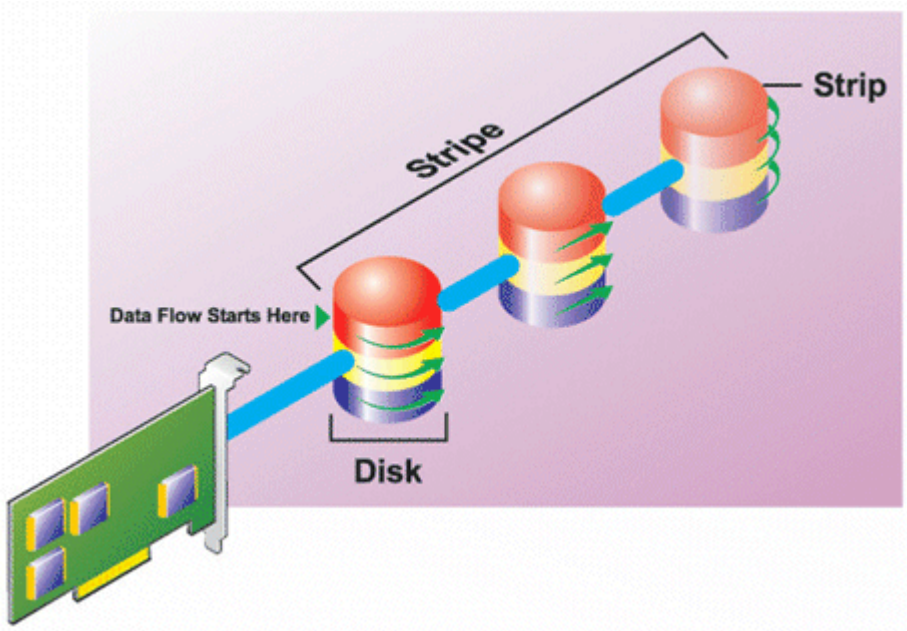


RAID 1

- Regroupe **n** + **n** disques en un seul disque virtuel d'une capacité de **n** disques. Les contrôleurs actuellement pris en charge par Storage Management permettent la sélection de deux disques lors de la création d'un RAID 1. Étant donné que ces disques sont mis en miroir, la capacité de stockage totale est égale à un disque.
- Les données sont répliquées sur les deux disques.
- Lorsqu'un disque est en échec, le disque virtuel continue de fonctionner. Les données sont lues à partir du miroir du disque en échec.
- Meilleures performances de lecture, mais performances d'écriture légèrement plus lentes.
- Redondance pour la protection des données.
- RAID 1 est plus cher en matière d'espace disque étant donné que deux fois plus de disque qu'il n'est requis pour le stockage des données sans redondance sont utilisés.

Niveau de RAID 5 ou agrégation par bandes avec parité distribuée

RAID 5 assure la redondance des données en utilisant l'agrégation par bandes des données en combinaison avec les informations de parité. Plutôt que de dédier un disque physique à la parité, les informations de parité sont réparties sur tous les disques physiques du groupe de disques.

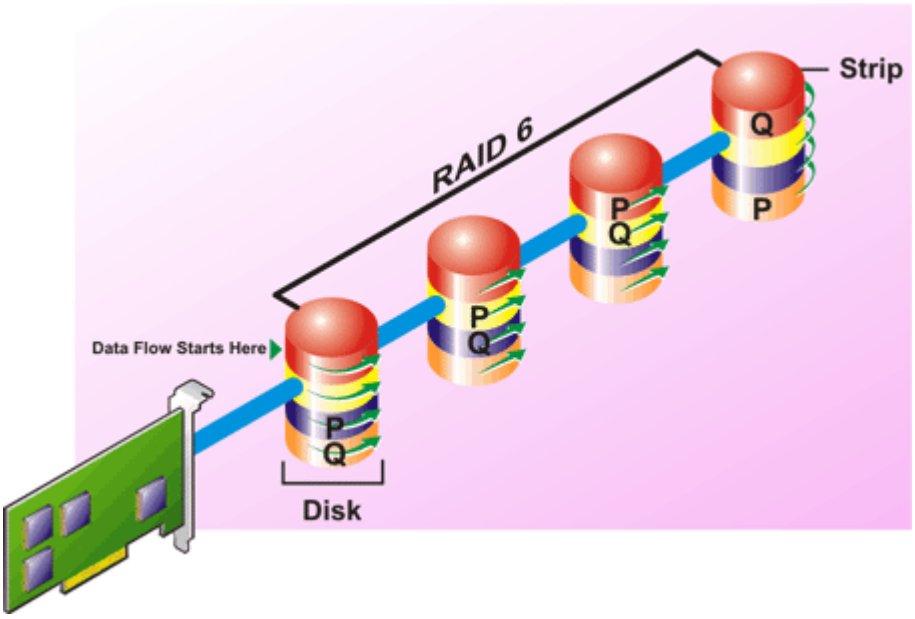


RAID 5

- Disques des groupes **n** comme disque virtuel important d'une capacité de (**n**-1) disques.
- Les informations redondantes (parité) sont stockées de manière alternative sur tous les disques.
- Lorsqu'un disque est en échec, le disque virtuel continue de fonctionner, mais il fonctionne dans un état dégradé. Les données sont reconstruites à partir des disques restants.
- Meilleures performances de lecture, mais performances d'écriture plus lentes.
- Redondance pour la protection des données.

Niveau de RAID 6 - Agrégation par bandes avec parité distribuée supplémentaire

RAID 6 assure la redondance des données en utilisant l'agrégation par bandes des données en combinaison avec les informations de parité. À l'instar du niveau RAID 5, la parité est distribuée dans chaque répartition. Le niveau RAID 6 utilise néanmoins un disque physique supplémentaire pour assurer la parité, de sorte que chaque répartition du groupe de disques conserve les informations de parité sur deux blocs de disque. La parité supplémentaire assure la protection des données en cas de panne de deux disques. Dans l'image suivante, les deux ensembles d'informations de parité sont identifiés comme **P** et **Q**.



RAID 6

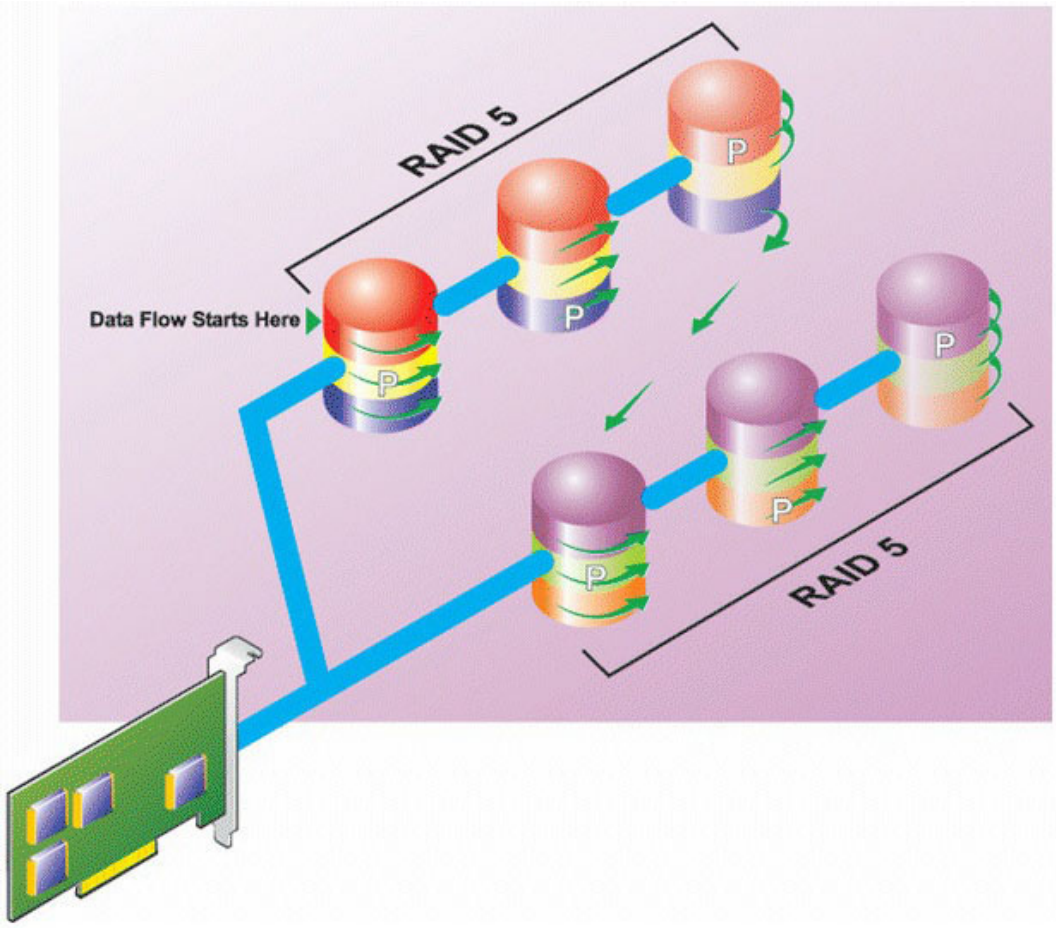
- Disques des groupes **n** comme disque virtuel important d'une capacité de (**n**-2) disques.

- Les informations redondantes (parité) sont stockées de manière alternative sur tous les disques.
- Le disque virtuel reste fonctionnel même si deux disques, au maximum, sont en panne. Les données sont reconstruites à partir des disques restants.
- Meilleures performances de lecture, mais performances d'écriture plus lentes.
- Redondance accrue pour la protection des données.
- Deux disques par répartition sont requis pour la parité. RAID 6 est plus onéreux en termes d'espace disque.

Niveau de RAID 50 - agrégation par bandes sur des ensembles RAID 5

RAID 50 est agrégé par bandes sur plusieurs répartitions de disques physiques. Par exemple, un groupe de disques RAID 5 qui est implémenté avec trois disques physiques, puis continue avec un groupe de disques composé de trois disques physiques supplémentaires est un RAID 50.

Il est possible d'implémenter RAID 50 même lorsque le matériel ne le prend pas en charge directement. Dans ce cas, vous pouvez implémenter plusieurs disques virtuels RAID 5, puis convertir les disques RAID 5 en disques dynamiques. Vous pouvez ensuite créer un volume dynamique réparti sur tous les disques virtuels RAID 5.

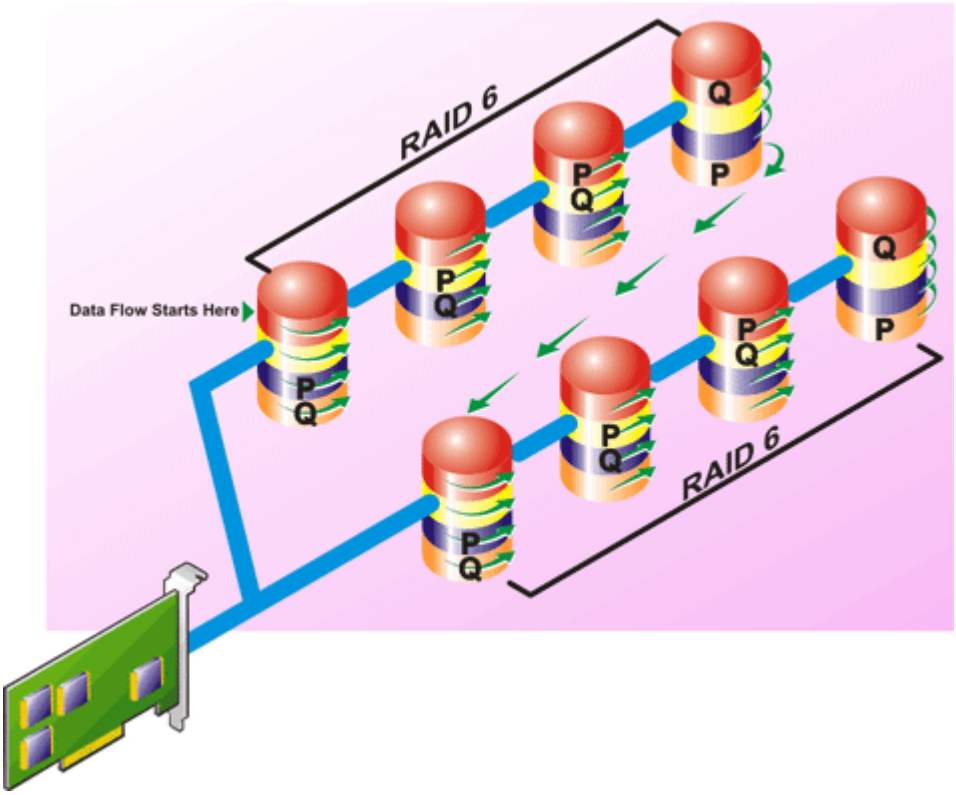


RAID 50

- Regroupe **n*****s** disques comme grand disque virtuel avec une capacité de **s***(**n**-1), où **s** correspond au nombre de répartitions et **n** au nombre de disques sur chaque répartition.
- Les informations redondantes (parité) sont stockées de manière alternative sur tous les disques de chaque répartition RAID 5.
- Meilleures performances de lecture, mais performances d'écriture plus lentes.
- Nécessite autant d'informations de parité que RAID 5 standard.
- Les données sont agrégées sur toutes les répartitions. RAID 50 est plus onéreux en termes d'espace disque.

Niveau de RAID 60 - agrégation par bandes sur des ensembles RAID 6

RAID 60 est agrégé par bandes sur plusieurs répartitions de disques physiques configurés en tant que RAID 6. Par exemple, un groupe de disques RAID 6 qui est implémenté avec quatre disques physiques, puis continue avec un groupe de disques composé de quatre disques physiques supplémentaires est un RAID 60.

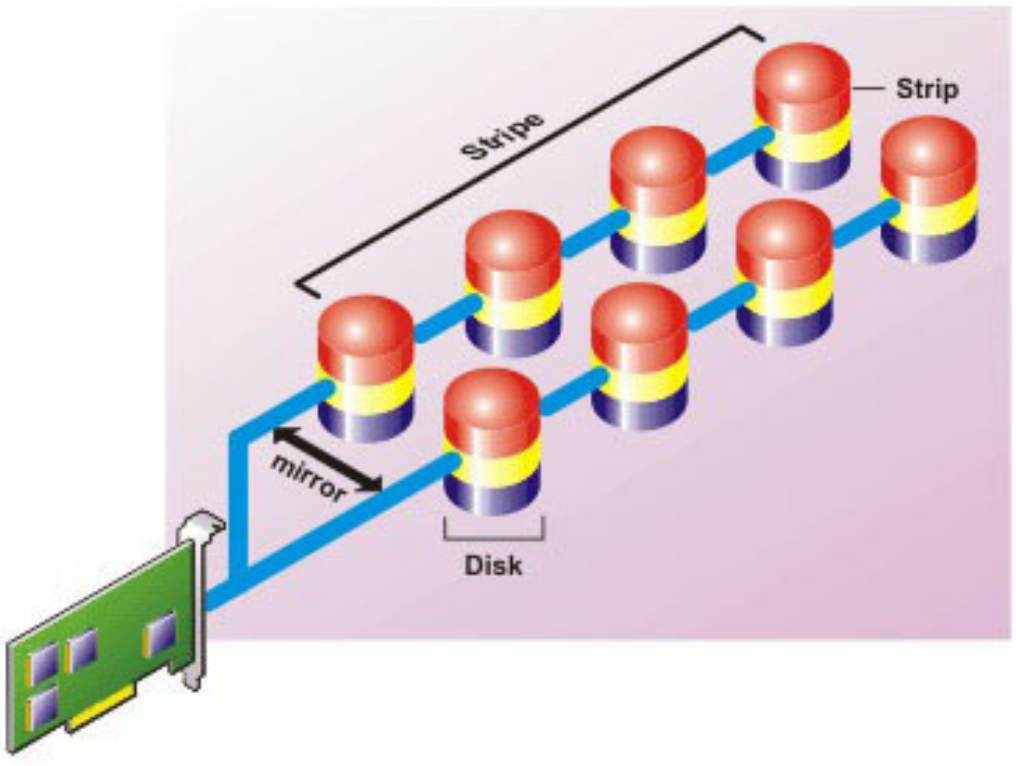


RAID 60

- Regroupe **n*****s** disques comme grand disque virtuel avec une capacité de **s***(**n**-2), où **s** correspond au nombre de répartitions et **n** au nombre de disques sur chaque répartition.
- Les informations redondantes (parité) sont stockées de manière alternative sur tous les disques de chaque répartition RAID 6.
- Meilleures performances de lecture, mais performances d'écriture plus lentes.
- Une redondance accrue fournit une protection des données plus importante qu'un RAID 50.
- Nécessite (proportionnellement) autant d'informations de parité que RAID 6.
- Deux disques par répartition sont requis pour la parité. RAID 60 est plus onéreux en termes d'espace disque.

Niveau de RAID 10 - miroirs répartis

Le RAB considère le niveau de RAID 10 comme une mise en œuvre du niveau de RAID 1. RAID 10 combine les disques physiques en miroir (RAID 1) et l'agrégation par bandes des données (RAID 0). Avec RAID 10, les données sont réparties sur plusieurs disques physiques. Le groupe de disques répartis est ensuite mis en miroir sur un autre ensemble de disques physiques. RAID 10 peut être considéré comme un **miroir de répartitions**.



RAID 10

- Regroupe **n** disques comme un grand disque virtuel avec une capacité de (**n**/2) disques, où **n** est un nombre entier pair.
- Les images miroirs des données sont réparties sur plusieurs ensembles de disques physiques. Ce niveau assure la redondance par la mise en miroir.
- Lorsqu'un disque est en échec, le disque virtuel continue de fonctionner. Les données sont lues à partir du disque en miroir restant.
- Meilleures performances de lecture et d'écriture.
- Redondance pour la protection des données.

Comparaison des performances des niveaux RAID

Le tableau suivant compare les caractéristiques des performances associées aux niveaux de RAID standard. Ce tableau fournit des consignes générales pour la sélection d'un niveau de RAID. Évaluez les exigences environnementales spécifiques de votre système avant de sélectionner un niveau de RAID.

Tableau 42. Comparaison des performances des niveaux RAID

Adresse RAID	Redondance des données	Performances de lecture	Performances d'écriture	Performances de recréaction	Nombre minimal de disques requis	Usages suggérés
RAID 0	Aucun	Très bon	Très bon	S/O	N	Données non critiques
RAID 1	Excellent	Très bon	Bon	Bon	2N (N = 1)	Petites bases de données, journaux de base de données et informations stratégiques.
RAID 5	Bon	Lectures séquentielles : bon. Lecture transactionnelles : Très bon	Bien, sauf si vous utilisez le cache d'écriture différée	Acceptable	N + 1 (N = au moins deux disques)	Pour les bases de données et d'autres usages transactionnels

Tableau 42. Comparaison des performances des niveaux RAID (suite)

Adresse RAID	Redondance des données	Performances de lecture	Performances d'écriture	Performances de recréaction	Nombre minimal de disques requis	Usages suggérés
						intensifs de lecture
RAID 10	Excellent	Très bon	Acceptable	Bon	2N x X	Environnements intensifs de données (enregistrements importants)
RAID 50	Bon	Très bon	Acceptable	Acceptable	N + 2 (N = au moins 4)	Environnements transactionnels de taille moyenne ou usages de données intensifs
RAID 6	Excellent	Lectures séquentielles : bon. Lecture transactionnelles : Très bon	Bien, sauf si vous utilisez le cache d'écriture différée	Médiocre	N + 2 (N = au moins deux disques)	Informations stratégiques. Pour les bases de données et d'autres usages transactionnels intensifs de lecture
RAID 60	Excellent	Très bon	Acceptable	Médiocre	X x (N + 2) (N = au moins 2)	Informations stratégiques. Environnements transactionnels de taille moyenne ou usages de données intensifs
N = nombre de disques physiques et X = nombre d'ensembles RAID						

Contrôleurs pris en charge

Contrôleurs RAID pris en charge

Les interfaces iDRAC prennent en charge les contrôleurs PERC12 suivants :

- PERC H965i avant
- PERC H965e

Les interfaces de l'iDRAC prennent en charge le contrôleur BOSS suivant :

- BOSS-N1

Boîtiers pris en charge

iDRAC prend en charge les boîtiers MD1400 et MD1420..

Récapitulatif des fonctionnalités prises en charge pour les périphériques de stockage

Les tableaux suivants fournissent les fonctionnalités prises en charge par les périphériques de stockage par le biais d'iDRAC.

Tableau 43. Fonctionnalités prises en charge pour les contrôleurs de stockage - PERC 12

Fonctionnalités	H965i Front et adaptateur H965i	Adaptateur H965e	Adaptateur H465i
Affecter ou annuler l'affectation d'un disque physique comme disque de secours global	En temps réel	En temps réel	Non applicable
Convertir en RAID	Non applicable	Sans objet	Sans objet
Convertir en RAID/non RAID,	En temps réel (convertit le disque en volume non RAID)	En temps réel (convertit le disque en volume non RAID)	En temps réel
Reconstruction	En temps réel	En temps réel	Non applicable
Annuler la recréation	En temps réel	En temps réel	Non applicable
Créer des disques virtuels	En temps réel	En temps réel	Non applicable
Renommer des disques virtuels	En temps réel	En temps réel	Non applicable
Modifiez les stratégies de cache des disques virtuels	En temps réel	En temps réel	Non applicable
Vérifiez la cohérence du disque virtuel	En temps réel	En temps réel	Non applicable
Annuler la vérification de la cohérence	Non applicable	Sans objet	Sans objet
Initialiser des disques virtuels	En temps réel	En temps réel	Non applicable
Annuler l'initialisation	En temps réel	En temps réel	Non applicable
Chiffrer des disques virtuels	En temps réel	En temps réel	Non applicable
Affectez ou annulez l'affectation d'un disque de secours dédié	En temps réel	En temps réel	Non applicable
Supprimer des disques virtuels	En temps réel	En temps réel	Non applicable
Annuler l'initialisation en arrière-plan	En temps réel	En temps réel	Non applicable
Extension de capacité en ligne	Non applicable	Sans objet	Sans objet
Migration de niveau de RAID	Non applicable	Sans objet	Sans objet
Suppression du cache conservé	En temps réel	En temps réel	En temps réel
Définir le mode de lecture cohérente	Non applicable	Sans objet	Sans objet
Mode de lecture cohérente manuel	En temps réel	En temps réel	Non applicable
Zones non configurées de la lecture cohérente	En temps réel	En temps réel	Non applicable
Mode de vérification de la cohérence	Non applicable	Sans objet	Sans objet
Mode de recopie	Non applicable	Sans objet	Sans objet
Mode d'équilibrage de charge	Non applicable	Sans objet	En temps réel

Tableau 43. Fonctionnalités prises en charge pour les contrôleurs de stockage - PERC 12 (suite)

Fonctionnalités	H965i Front et adaptateur H965i	Adaptateur H965e	Adaptateur H465i
Taux de vérification de la cohérence	En temps réel	En temps réel	Non applicable
VD de démarrage	Non applicable	Non applicable	Sans objet
Modifier l'état du disque physique	Non applicable	Sans objet	En temps réel
Taux de recréation	En temps réel	En temps réel	Non applicable
Taux d'initialisation en arrière-plan (BGI)	En temps réel	En temps réel	Non applicable
Taux de reconstruction	En temps réel	En temps réel	Non applicable
Importer la configuration étrangère	En temps réel	En temps réel	Non applicable
Importer automatiquement une configuration étrangère	Non applicable	Sans objet	Sans objet
Effacer la configuration étrangère	En temps réel	En temps réel	Non applicable
Réinitialiser la configuration d'un contrôleur	En temps réel	En temps réel	Non applicable
Créez ou modifiez les clés de sécurité	En temps réel	En temps réel	En temps réel
Secure Enterprise Key Manager	En temps réel	En temps réel	En temps réel
Faire l'inventaire et surveiller à distance l'intégrité des périphériques SSD PCIe	Non applicable	Sans objet	Sans objet
Préparez le retrait du SSD PCIe	Non applicable	Sans objet	Sans objet
Effacer les données en toute sécurité pour le disque SSD PCIe	Non applicable	Sans objet	En temps réel
Configurer le mode du fond de panier (fractionné/unifié)	En temps réel	En temps réel	Non applicable
Faites clignoter ou annulez le clignotement des LED des composants	En temps réel	En temps réel	En temps réel
Basculer le mode du contrôleur	Non applicable	Sans objet	Sans objet
Prise en charge de T10PI pour les disques virtuels	Non applicable	Sans objet	Sans objet

Tableau 44. fonctionnalités prises en charge pour les périphériques de stockage

Fonctionnalité	BOSS-N1
Créer des disques virtuels	Simulé
Réinitialiser la configuration d'un contrôleur	Simulé
Initialisation rapide	Simulé
Supprimer des disques virtuels	Simulé

Tableau 44. fonctionnalités prises en charge pour les périphériques de stockage (suite)

Fonctionnalité	BOSS-N1
Initialisation complète	Non applicable
Faire l'inventaire et surveiller à distance l'intégrité des périphériques SSD PCIe	Non applicable
Préparez le retrait du SSD PCIe	Non applicable
Effacer les données en toute sécurité pour le disque SSD PCIe	Non applicable
Faites clignoter ou annulez le clignotement des LED des composants	En temps réel
Connexion à chaud des disques	En temps réel
SEKM	Simulé
Niveaux RAID pris en charge	RAID 0 et RAID 1

Inventaire et surveillance des périphériques de stockage

Vous pouvez surveiller à distance l'intégrité et afficher l'inventaire des périphériques de stockage CEM (Comprehensive Embedded Management) suivants dans le système géré à l'aide de l'interface web d'iDRAC :

- Contrôleurs RAID, contrôleurs non RAID, contrôleurs BOSS et cartes d'extension PCIe
- Boîtiers contenant des modules EMM (Enclosure Management Modules), un bloc d'alimentation, un capteur de ventilateur et un capteur de température.
- Disques physiques
- disques virtuels
- Batteries

REMARQUE :

- Sur un système avec plus de disques virtuels, l'inventaire du matériel peut afficher des données de disques physiques vides pour certains disques virtuels.
- Des alertes et des interruptions SNMP sont générées pour les événements de stockage. Les événements sont consignés dans le journal Lifecycle.
- Si vous tentez de supprimer des tâches terminées d'une file d'attente de tâches lorsqu'une tâche est en cours, celle qui est en cours peut échouer. Par conséquent, il est recommandé d'attendre la fin de la tâche en cours avant de les supprimer.
- Pour un inventaire précis des contrôleurs BOSS, assurez-vous que l'opération CSIOR (Collect System Inventory On Reboot Operation) est terminée. CSIOR est activé par défaut.
- Les disques physiques d'un système comprenant plusieurs fonds de paniers peuvent être répertoriés sous un autre fond de panier. Utilisez la fonction clignotement pour identifier les disques.
- Le FQDD de certains fonds de panier peut ne pas être identique dans l'inventaire des logiciels et l'inventaire du matériel.
- Le journal Lifecycle pour le contrôleur PERC n'est pas disponible lorsque les événements du contrôleur PERC précédents sont traités. Cela n'affecte pas le fonctionnement. Le traitement des événements passés peut varier en fonction de la configuration.
- Lors du retrait à chaud du disque M.2 du contrôleur BOSS N1, l'état d'intégrité du tableau de bord de l'iDRAC devient orange, mais le voyant LED d'intégrité avant/arrière du serveur reste bleu.

REMARQUE : Vous pouvez voir l'erreur SRV015 dans deux cas : lorsque l'appareil ne prend pas en charge la collecte TSR comme les contrôleurs AHCI ou si l'appareil prend en charge la collecte TSR, mais n'est pas encore inventorié sur la bande latérale.

Surveillance des périphériques de stockage à l'aide de l'interface Web

Pour afficher les informations des périphériques de stockage en utilisant l'interface Web :

- Accédez à **Stockage** > **Présentation** > **Récapitulatif** pour afficher le récapitulatif des composants de stockage et les derniers événements consignés. Cette page est automatiquement actualisée toutes les 30 secondes.
- Accédez à **Stockage** > **Présentation** > **Contrôleurs** pour afficher les informations relatives aux contrôleurs RAID. La page **Contrôleurs** s'affiche.

- Accédez à **Stockage** > **Présentation** > **Disques physiques** pour afficher les informations relatives aux disques physiques. La page **Disques physiques** s'affiche.
- Accédez à **Stockage** > **Présentation** > **Disques virtuels** pour afficher les informations relatives aux disques virtuels. La page **Disques virtuels** s'affiche.
- Accédez à **Stockage** > **Présentation** > **Boîtiers** pour afficher les informations relatives aux boîtiers. La page **Boîtiers** s'affiche.

REMARQUE : Si le serveur comprend un nombre impair de logements, une ligne de logements vide est ajoutée dans la liste **Résumé des logements** de la page **Boîtier**.

REMARQUE : Pour plus d'informations sur les propriétés prises en charge et leurs valeurs, consultez l'**aide en ligne de l'iDRAC**.

Vous pouvez également utiliser des filtres pour afficher les informations relatives à des périphériques spécifiques.

REMARQUE :

- La liste du matériel de stockage ne s'affiche pas si le système ne contient aucune unité de stockage avec prise en charge CEM.
- Il est possible que le comportement des appareils NVMe non Dell certifiés ou tiers ne soit pas cohérent dans l'iDRAC.
- Si les disques SSD NVMe dans les logements de fond de panier prennent en charge les commandes NVMe-MI et que la connexion I2C aux logements de fond de panier est satisfaisante, le contrôleur iDRAC découvre ces SSD NVMe et les signale dans les interfaces, quelles que soient les connexions PCI aux logements de fond de panier respectifs.

REMARQUE :

Tableau 45. Prise en charge de l'interface utilisateur et d'autres interfaces

Type	Prise en charge des interfaces utilisateur graphiques Web	Autres interfaces prises en charge
SATA	Non disponible	Inventaire et configuration RAID
NVMe	Inventaire de disques physiques uniquement	Inventaire et configuration RAID

Pour plus d'informations sur les propriétés affichées et l'utilisation des options, voir l'Aide en ligne d'iDRAC.

Surveillance d'un périphérique de stockage à l'aide de l'interface RACADM

Pour afficher les informations sur un périphérique de stockage, utilisez la commande `storage`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Surveillance d'un fond de panier à l'aide de l'utilitaire de paramètres d'iDRAC

Dans l'utilitaire de configuration de l'iDRAC, accédez à **Récapitulatif du système**. La page **Paramètres iDRAC-Récapitulatif du système** s'affiche. La section **Inventaire du fond de panier** affiche les informations relatives au fond de panier. Pour plus d'informations sur les champs, voir l'**Aide en ligne de l'utilitaire de configuration d'iDRAC**.

Affichage de la topologie des périphériques de stockage

Utilisez cette page pour afficher la vue hiérarchique du confinement physique des principaux composants de stockage. Cette page répertorie les contrôleurs, les boîtiers connectés au contrôleur et un lien vers le disque physique contenu dans chaque boîtier. Les disques physiques connectés directement au contrôleur sont également affichés.

Pour afficher la topologie des périphériques de stockage, accédez à **Stockage** > **Présentation**. La page **Présentation** contient une représentation hiérarchique des composants de stockage du système. Les options disponibles sont les suivantes :

- Contrôleurs
- Disques physiques

- Disques virtuels.
- Boîtiers

Cliquez sur les liens pour afficher les détails des composants respectifs.

Gestion des disques physiques

Vous pouvez effectuer les tâches suivantes pour les disques physiques :

- Afficher les propriétés d'un disque physique.
- Affecter ou annuler l'affectation d'un disque physique comme disque de secours global.
- Convertir en disque RAID.
- Convertir en disque non RAID.
- Faire clignoter le voyant LED ou arrêter son clignotement.
- Recréation d'un disque physique
- Annuler la recréation d'un disque physique
- Effacement cryptographique

REMARQUE : Si l'un des disques sécurisés SEKM qui sont directement connectés au serveur ou derrière un contrôleur n'est pas visible ou accessible par le système d'exploitation, il est recommandé de consulter les journaux LC et de s'assurer que tous les disques sécurisés sont déverrouillés. Sinon, prenez les mesures recommandées dans les journaux LC.

Affectation ou annulation de l'affectation de disques de secours dédiés

Un disque de secours dédié est un disque de sauvegarde inutilisé attribué à un disque virtuel. Lorsqu'un disque physique du disque virtuel échoue, le disque de secours est activé pour remplacer le disque physique problématique sans que le système ne soit interrompu ou que votre intervention ne soit requise

Vous devez disposer des privilèges de contrôle du serveur et d'ouverture de session pour exécuter cette opération.

Vous pouvez affecter uniquement des disques 4K en tant que disques de secours à des disques virtuels 4K.

Si vous avez affecté un disque physique en tant que disque de secours dédié en mode Ajouter à l'opération en attente, l'opération en attente est créée, mais pas la tâche. Si vous tentez ensuite d'annuler l'affectation du disque de secours dédié, l'opération en attente d'affectation de disque de secours dédié est désactivée.

Si vous avez annulé l'affectation d'un disque physique en tant que disque de secours dédié en mode Ajouter à l'opération en attente, l'opération en attente est créée, mais pas la tâche. Si vous tentez ensuite d'affecter le disque de secours dédié, l'opération en attente d'annulation d'affectation de disque de secours dédié est désactivée.

REMARQUE : Lorsque l'opération d'exportation du journal est en cours, vous ne pouvez pas afficher d'informations sur les disques de secours dédiés sur la page **Gérer les disques virtuels**. Une fois l'opération d'exportation du journal terminée, rechargez ou actualisez la page **Gérer les disques virtuels** pour afficher les informations.

Affectation ou annulation de l'affectation d'un disque de secours global à l'aide de l'interface Web

Pour affecter ou annuler l'affectation d'un disque de secours global pour un lecteur de disque physique :

1. Dans l'interface Web d'iDRAC, accédez à **Stockage** > **Présentation** > **Disques physiques**.
2. Tous les disques physiques disponibles s'affichent.
3. Pour affecter un disque en tant que disque de secours global, dans les menus déroulants de la colonne **Action**, sélectionnez **Attribuer un disque de secours global** pour un ou plusieurs disques physiques.
4. Pour annuler l'affectation d'un disque de secours global, dans les menus déroulants de la colonne **Action**, sélectionnez **Annuler l'affectation d'un disque de rechange** pour un ou plusieurs disques physiques.
5. Cliquez sur **Appliquer maintenant**.
   En fonction de vos besoins, vous pouvez également choisir d'appliquer **Au prochain redémarrage** ou **À l'heure planifiée**. Les paramètres sont appliqués en fonction du mode de fonctionnement sélectionné.

Affectation ou annulation de l'affectation d'un disque de secours global à l'aide de RACADM

Utilisez la commande `storage`et indiquez le type de stockage comme disque de secours global.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Conversion d'un disque physique au mode RAID ou non RAID

La conversion d'un disque physique au mode RAID active le disque pour toutes les opérations RAID. Lorsqu'un disque est en mode non RAID, il est exposé au système d'exploitation contrairement aux bons disques non configurés et est utilisé en mode de transmission directe.

Vous pouvez convertir les disques physiques en disques RAID ou non RAID :

- En utilisant les interfaces de l'iDRAC telles que l'interface Web, RACADM ou Redfish.
- En appuyant sur la combinaison de touches <Ctrl+R> lors du redémarrage du serveur, puis en sélectionnant le contrôleur requis.

REMARQUE : Si les lecteurs physiques connectés à un contrôleur PERC sont en mode non RAID, la taille du disque affichée dans les interfaces iDRAC, comme l'interface graphique iDRAC, RACADM et Redfish, peut être légèrement inférieure à la taille réelle du disque. Cependant, vous pouvez utiliser toute la capacité du disque pour déployer des systèmes d'exploitation.

Conversion de disques physiques en disques RAID ou non RAID à l'aide de l'interface Web iDRAC

Pour convertir les disques physiques en mode RAID ou non RAID, effectuez les opérations suivantes :

1. Dans l'interface Web d'iDRAC, cliquez sur **Stockage** > **Présentation** > **Disques physiques**.
2. Cliquez sur **Options de filtre**. Deux options s'affichent : **Effacer tous les filtres** et **Filtre avancé**. Cliquez sur l'option **Filtre avancé**.
   Une liste élaborée s'affiche et vous permet de configurer différents paramètres.
3. Dans le menu déroulant **Regrouper par**, sélectionnez un boîtier ou des disques virtuels.
   Les paramètres associés au boîtier ou aux disques virtuels s'affichent.
4. Cliquez sur **Appliquer** une fois que vous avez sélectionné tous les paramètres souhaités. Pour plus d'informations sur les champs, voir l'**Aide en ligne de l'iDRAC**.
   Les paramètres sont appliqués en fonction de l'option sélectionnée dans le mode de fonctionnement.

Conversion de disques physiques au mode RAID ou non RAID à l'aide de RACADM

Selon que vous souhaitez effectuer une conversion au mode RAID ou non RAID, utilisez les commandes RACADM suivantes :

- Pour effectuer une conversion au mode RAID, utilisez la commande `racadm storage converttoraid`.
- Pour procéder à une conversion au mode non RAID, utilisez la commande `racadm storage converttononraid`.

REMARQUE : Sur le contrôleur S140, vous ne pouvez utiliser que l'interface RACADM pour convertir les disques du mode non-RAID au mode RAID. Les modes RAID logiciels pris en charge sont les modes Windows ou Linux.

Pour plus d'informations sur les commandes, voir leGuide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Effacement des disques physiques

La fonctionnalité System Erase permet d'effacer le contenu des disques physiques. Cette fonctionnalité est accessible à l'aide de RACADM ou de l'interface utilisateur de LC. Les disques physiques du serveur sont regroupés en deux catégories.

- Disques à effacement sécurisé : inclut les disques qui fournissent l'effacement du chiffrement, tel que les disques ISE, SED SAS, SATA et SSD PCIe.

REMARQUE : Les disques ISE respectent la norme NIST SP 800-88r1 et sont conformes à la purge NIST. Cela signifie que toutes les **anciennes données** sont irrécupérables après effacement.

- Disques à effacement par écrasement : inclut tous les disques qui ne prennent pas en charge l'effacement du chiffrement.

REMARQUE : L'option d'effacement du système s'applique uniquement aux disques du serveur. L'iDRAC ne peut pas effacer les disques d'un boîtier externe tel qu'un JBOD.

La sous-commande RACADM SystemErase inclut des options pour les catégories suivantes :

- L'option **SecureErasePD** efface de manière cryptographique tous les disques à effacement sécurisé.
- L'option **OverwritePD** écrase les données sur tous les disques.

REMARQUE : L'effacement cryptographique des disques physiques BOSS peut être effectué par la méthode `SystemErase` et il est pris en charge à partir de l'interface utilisateur de LC et de RACADM.

Avant de procéder à SystemErase, utilisez la commande suivante pour vérifier la fonctionnalité d'effacement de tous les disques physiques d'un serveur :

```
# racadm storage get pdisks -o -p SystemEraseCapability
```

REMARQUE : Si SEKM est activé sur le serveur, désactivez-le à l'aide de la commande `racadm sekm disable` avant d'utiliser cette commande. Cela peut empêcher le verrouillage de tous les appareils de stockage sécurisés par l'iDRAC si les paramètres SEKM sont effacés de l'iDRAC en exécutant cette commande.

Pour effacer des disques ISE et SED, utilisez cette commande :

```
# racadm systemerase -secureerasepd
```

Pour effacer des disques à effacement par écrasement, utilisez la commande suivante :

```
# racadm systemerase -overwritepd
```

REMARQUE : RACADM SystemErase supprime tous les disques virtuels des disques physiques qui sont effacés par les commandes ci-dessus.

REMARQUE : RACADM SystemErase provoque le redémarrage du serveur pour pouvoir effectuer les opérations d'effacement.

REMARQUE : Les disques SSD ou SED PCIe peuvent être effacés à l'aide de l'interface utilisateur de l'iDRAC ou de RACADM. Pour plus d'informations, voir les sections Effacement des données d'un périphérique SSD PCIe et Effacement des données d'un périphérique SED à l'aide de l'interface utilisateur.

Pour plus d'informations sur la fonction System Erase dans l'interface utilisateur de Lifecycle Controller, voir le *Guide de l'utilisateur de Dell Lifecycle Controller* disponible à l'adresse des manuels iDRAC.

Effacement des données d'un périphérique SED/ISE

REMARQUE : Cette opération n'est pas prise en charge lorsque le périphérique pris en charge fait partie d'un disque virtuel. Le périphérique cible pris en charge doit être supprimé du disque virtuel avant de pouvoir effectuer l'effacement du contenu du périphérique.

La tâche Effacement du chiffrement efface définitivement toutes les données présentes sur le disque. Tout effacement du chiffrement sur un disque SED/ISE écrase tous les blocs et entraîne la perte définitive de toutes les données présentes sur les périphériques pris en charge. Pendant l'effacement du chiffrement, l'hôte ne peut pas accéder au périphérique pris en charge. L'effacement des données du périphérique SED/ISE peut être effectué en temps réel ou être appliqué après un redémarrage du système.

Si le système redémarre ou subit une panne d'alimentation au cours d'un effacement du chiffrel, l'opération est annulée. Vous devez redémarrer le système et recommencer le processus.

Avant d'effacer les données d'un périphérique SED/ISE, vérifiez les points suivants :

- Le Lifecycle Controller est activé.
- Vous disposez des privilèges de contrôle et d'ouverture de session sur le serveur.
- Le disque pris en charge que vous avez sélectionné ne fait pas partie d'un disque virtuel.

REMARQUE :

- L'effacement des données d'un périphérique SED/ISE peut être effectué en temps réel ou dans le cadre d'une opération progressive.
- Une fois le disque effacé, il peut toujours apparaître comme actif dans le système d'exploitation en raison de la mise en cache des données. Si cela se produit, redémarrez le système d'exploitation pour que le disque effacé ne s'affiche plus ou ne génère plus aucune donnée.
- L'opération d'effacement du chiffrement n'est pas prise en charge pour les disques NVMe connectés à chaud. Redémarrez le serveur avant de démarrer l'opération. Si l'opération continue d'échouer, assurez-vous que CSIOR est activé et que les disques NVMe sont qualifiés par Dell Technologies.
- L'effacement cryptographique peut également être effectué à l'aide de PSID.

Effacement des données d'un périphérique SED à l'aide de RACADM

Pour effacer en toute sécurité un périphérique SED :

```
racadm storage cryptographicerase:<SED FQDD>
```

Pour créer la tâche cible après avoir exécuté la commande `cryptographicerase` :

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -realtime
```

Pour créer la tâche cible planifiée après avoir exécuté la commande cryptographicerase :

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -e <start_time>
```

Pour rechercher l'ID de tâche renvoyée :

```
racadm jobqueue view -i <job ID>
```

Pour réaliser l'effacement cryptographique :

```
<SED FQDD> -psid<PSID>
```

Pour en savoir plus, voir le *Guide de la CLI RACADM de l'iDRAC (Integrated Dell Remote Access Controller)*.

Effacement des données d'un périphérique SED/ISE à l'aide de l'interface Web

Pour effacer les données sur le périphérique pris en charge :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Disques physiques**.
   La page **Disques physiques** s'affiche.
2. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur pour afficher les périphériques associés.
3. Dans les menus déroulants, sélectionnez **Effacement cryptographique** pour un ou plusieurs périphériques SED/ISE.
   Si vous avez sélectionné **Effacement cryptographique** et que vous souhaitez afficher les autres options du menu déroulant, sélectionnez **Action**, puis cliquez sur le menu déroulant pour afficher les autres options.
4. Dans le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez l'une des options suivantes :
   - **Appliquer maintenant** : sélectionnez cette option pour appliquer immédiatement les actions sans avoir à redémarrer le système.
   - **Au prochain redémarrage** : cette option permet d'appliquer les actions lors du prochain redémarrage système.
   - **À l'heure programmée** : sélectionnez cette option pour appliquer les actions à un jour et à une heure planifiés :
     - **Heure de début** et **Heure de fin** : cliquez sur les icônes de calendrier et sélectionnez les dates. Dans les menus déroulants, sélectionnez l'heure. L'action est appliquée entre l'heure de début et l'heure de fin.
     - Dans le menu déroulant, sélectionnez le type de redémarrage :
       - Pas de redémarrage (Redémarrage manuel du système)
       - Arrêt normal
       - Arrêt forcé

- Exécuter un cycle d'alimentation du système (démarrage à froid)

5. Cliquez sur **Appliquer**.

   Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué s'affiche. De plus, l'ID du message et l'action de réponse recommandée s'affichent.

   Si la tâche est créée avec succès, un message indiquant que l'ID de tâche est créée sur le contrôleur sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page File d'attente.

   Si l'opération en attente n'est pas créée, un message d'erreur s'affiche. Si l'opération en attente aboutit mais que la création de la tâche échoue, un message d'erreur s'affiche.

Recréation d'un disque physique

La reconstruction d'un disque physique permet de reconstituer le contenu d'un disque défaillant. Cela n'est possible que si l'option de reconstruction automatique est définie sur False. S'il existe un disque virtuel redondant, l'opération de reconstruction peut reconstituer le contenu d'un disque physique défaillant. Une reconstruction peut se faire en cours de fonctionnement normal, mais elle affecte les performances.

Vous pouvez utiliser la fonction d'annulation d'une reconstruction pour annuler une reconstruction en cours. Si vous annulez une reconstruction, le disque virtuel reste dans un état dégradé. L'échec d'un disque physique supplémentaire peut entraîner l'échec du disque virtuel et entraîner une perte de données. Il est recommandé d'effectuer une reconstruction sur le disque physique défaillant au plus tôt.

Si vous annulez la reconstruction d'un disque physique attribué comme disque de secours, relancez la reconstruction sur le même disque physique afin de restaurer les données. Si vous annulez la recréation d'un disque physique, puis attribuez un autre disque physique comme disque de secours, le nouveau disque de secours ne recrée pas les données.

Gestion de disques virtuels

Vous pouvez effectuer les opérations suivantes pour les disques virtuels :

- Créer
- Supprimer
- Modifier les règles
- Initialize
- Vérifier la cohérence
- Annuler la vérification de la cohérence
- Chiffrer des disques virtuels
- Affecter ou annuler l'affectation de disques de secours dédiés
- Faire clignoter la LED et Arrêter le clignotement de la LED d'un disque virtuel
- Annuler l'initialisation en arrière-plan
- Extension de capacité en ligne
- Migration du niveau RAID

REMARQUE : Vous pouvez gérer et surveiller 240 disques virtuels à l'aide de l'interface de l'iDRAC. Pour créer des VDS, utilisez le paramétrage du périphérique (F2) ou l'outil de ligne de commande PERCCLI.

Création de disques virtuels

Pour mettre en œuvre des fonctionnalités RAID, vous devez créer un disque virtuel. Un disque virtuel correspond à l'espace de stockage créé par un contrôleur RAID à partir d'un ou de plusieurs disques physiques. Il est possible de créer un disque virtuel à partir de plusieurs disques physiques, mais le système d'exploitation le considère comme un disque unique.

Avant de créer un disque virtuel, vous devez vous familiariser avec les informations se trouvant dans la rubrique Considérations précédant la création de disques virtuels.

Vous pouvez créer un disque virtuel à partir des disques physiques rattachés au contrôleur PERC. Pour créer un disque virtuel, vous devez disposer du droit de contrôler le serveur. Vous pouvez créer au maximum 64 disques virtuels, avec un maximum de 16 disques par groupe.

Vous ne pouvez pas créer de disque virtuel si :

- Aucun disque physique n'est disponible pour la création de disques virtuels. Dans ce cas, ajoutez des disques physiques supplémentaires.
- Vous avez atteint le nombre maximal de disques virtuels pouvant être créés sur le contrôleur. Dans ce cas, vous devez supprimer au moins un disque virtuel pour pouvoir en créer un nouveau.
- Le nombre maximal de disques virtuels pris en charge par un groupe de disques a été atteint. Dans ce cas, vous devez supprimer un disque virtuel dudit groupe pour pouvoir en créer un nouveau.
- Une tâche est en cours d'exécution ou planifiée sur le contrôleur sélectionné. Vous devez attendre que cette tâche soit achevée ou vous pouvez la supprimer avant de tenter une nouvelle opération. Vous pouvez afficher et gérer le statut de la tâche planifiée dans la page File d'attente des tâches.
- Le disque physique est en mode non RAID. Dans ce cas, vous devez effectuer la conversion vers le mode RAID avec les interfaces iDRAC, notamment l'interface Web iDRAC, RACADM, Redfish ou <CTRL+R>.

REMARQUE : Si vous créez un disque virtuel en mode Ajouter à une opération en attente et qu'une tâche n'est pas créée, puis si vous supprimez le disque virtuel, l'opération de création de disque virtuel en attente est désactivée.

REMARQUE : Le contrôleur BOSS vous permet de créer un disque virtuel uniquement de taille égale à la taille complète du support de stockage physique M.2. Veillez à définir la taille du disque virtuel à zéro si vous utilisez le profil de configuration de serveur pour créer un disque virtuel BOSS. Pour les autres interfaces telles que RACADM et Redfish, la taille du disque virtuel ne doit pas être spécifiée.

REMARQUE : La création de disques virtuels n'est pas autorisée sur les disques déjà sécurisés.

Éléments à prendre en compte avant la création de disques virtuels

Avant la création des disques virtuels, tenez compte des éléments suivants :

- Noms des disques virtuels non stockés sur le contrôleur : les noms des disques virtuels que vous créez ne sont pas stockés sur le contrôleur. Cela signifie que si vous effectuez un redémarrage à l'aide d'un autre système d'exploitation, le nouveau système d'exploitation peut renommer le disque virtuel en utilisant ses propres conventions d'affectation de noms.
- Un groupe de disques est un groupement logique de disques reliés à un contrôleur RAID sur lequel un ou plusieurs disques virtuels sont créés de sorte que tous les disques virtuels du groupe de disques utilisent tous les disques physiques de ce groupe. La version actuelle prend en charge le blocage de groupes de disques mixtes lors de la création de périphériques logiques.
- Les disques physiques sont liés à des groupes de disques. Par conséquent, il n'y a aucune combinaison de niveaux de RAID sur un seul groupe de disques.
- Il existe des limites quant au nombre de disques physiques pouvant être inclus dans le disque virtuel. Ces limites dépendent du contrôleur. Lors de la création d'un disque virtuel, les contrôleurs prennent en charge certaines bandes et répartitions (méthodes permettant de combiner les ressources de stockage sur les disques physiques). Étant donné que le nombre total de bandes et de répartitions est limité, le nombre de disques physiques pouvant être utilisés est lui aussi limité. Les limites de bandes et de répartitions affectent les niveaux de RAID de la manière suivante :
  - Le nombre maximal de répartitions affecte les RAID 10, RAID 50 et RAID 60.
  - Le nombre maximal de bandes affecte les RAID 0, RAID 5, RAID 50, RAID 6 et RAID 60.
  - Le nombre de disques physiques dans un miroir est toujours de 2. Cela affecte les RAID 1 et RAID 10.

  REMARQUE :
  - RAID 1 et RAID 0 ne sont pris en charge que pour les contrôleurs BOSS.
  - Le contrôleur SWRAID prend uniquement en charge les niveaux RAID 0, 1, 5 et 10.
- Impossible de créer des disques virtuels sur les SSD PCIe. Mais les contrôleurs PERC 11 et versions ultérieures prennent en charge la création de disques virtuels à l'aide de disques SSD PCIe.

REMARQUE : Certaines actions peuvent empêcher la réinitialisation de l'ID cible de démarrage sur ffff lorsqu'aucun disque virtuel ou EPD-PT n'est configuré.

Création de disques virtuels à l'aide de RACADM

Utilisez la commande `racadm storage createvd`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

REMARQUE : Le sectionnement du disque ou la configuration de disques virtuels partiels n'est pas pris en charge à l'aide de RACADM sur disques gérés par le contrôleur S140.

Création de disques virtuels à l'aide de l'interface Web

Pour créer un disque virtuel :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Disques virtuelsFiltre avancé**.
2. Dans la section **Disque virtuel**, procédez comme suit :
   a. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur dont vous souhaitez créer le disque virtuel.
   b. Dans le menu déroulant **Disposition**, sélectionnez le niveau de RAID du disque virtuel :
      Seuls les niveaux de RAID pris en charge par le contrôleur s'affichent dans le menu déroulant et ce, en fonction du nombre total de disques physiques disponibles.
   c. Sélectionnez le **Type de média**, **Taille de répartition**, **Règle de lecture**, **Règles d'écriture** et **Règle de cache du disque**, .
      Seules les valeurs prises en charge par le contrôleur s'affichent dans les menus déroulants de ces propriétés.
   d. Dans le champ **Capacité**, spécifiez la taille du disque virtuel.
      La taille maximale est affichée, puis mise à jour à mesure que les disques sont sélectionnés.
   e. Le champ **Nombre des répartitions** s'affiche en fonction des disques physiques sélectionnés (étape 3). Vous ne pouvez pas définir cette valeur. Elle est calculée automatiquement après la sélection des disques pour le niveau multi-RAID. Le champ **Nombre des répartitions** s'applique uniquement à RAID 10, RAID 50 et RAID 60. Si vous avez sélectionné RAID 10 et si le contrôleur prend en charge la valeur RAID 10 impaire, alors la valeur du nombre de répartitions ne s'affiche pas. Le contrôleur définit automatiquement la valeur appropriée. Pour RAID 50 et RAID 60, ce champ ne s'affiche pas lorsque le nombre minimal de disques est utilisé pour créer RAID. Il peut être modifié si vous utilisez plus de disques.
3. Dans la section **Sélectionner les disques physiques**, sélectionnez le nombre de disques physiques.
   Pour plus d'informations sur les champs, voir l'**Aide en ligne de l'iDRAC**.
4. Depuis le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez appliquer les paramètres.
5. Cliquez sur **Créer un disque virtuel**.
   Les paramètres sont appliqués en fonction du **mode de fonctionnement** sélectionné.
   REMARQUE : Vous pouvez utiliser des caractères alphanumériques, des tirets et des traits de soulignement dans le nom du disque.

Modification des règles de cache des disques virtuels

Vous pouvez modifier les règles de lecture, d'écriture et de cache d'un disque virtuel.

REMARQUE : Certains contrôleurs ne prennent pas en charge toutes les règles de lecture ou d'écriture. Par conséquent, lorsqu'une règle est appliquée, un message d'erreur s'affiche.

Les règles de lecture indiquent si le contrôleur doit lire des secteurs séquentiels du disque virtuel lorsqu'il recherche des données.

- **Lecture anticipée adaptative** : le contrôleur lance la lecture anticipée uniquement si les requêtes de lecture les plus récentes ont accédé à des secteurs séquentiels du disque. Si les requêtes de lecture suivantes accèdent à des secteurs aléatoires du disque, le contrôleur applique de nouveau la règle Pas de lecture anticipée. Le contrôleur continue d'évaluer si les requêtes de lecture accèdent à des secteurs séquentiels du disque et lance la lecture anticipée si nécessaire.
- **Lecture anticipée** : le contrôleur lit les secteurs séquentiels du disque virtuel lorsqu'il recherche des données. La règle Lecture anticipée peut améliorer les performances du système si les données sont écrites dans les secteurs séquentiels du disque virtuel.
- **Sans lecture anticipée** : la sélection de la règle Sans lecture anticipée indique que le contrôleur ne doit pas utiliser la règle de lecture anticipée.

Les règles d'écriture spécifient si le contrôleur envoie un signal indiquant que la requête d'écriture est terminée dès que les données se trouvent en cache ou une fois qu'elles ont été écrites sur le disque.

- **Écriture immédiate** : le contrôleur envoie un signal d'achèvement de la requête d'écriture uniquement après l'écriture des données sur le disque. La mise en cache d'écriture immédiate offre un niveau de sécurité des données plus important que la mise en cache d'écriture différée, car le système considère que les données sont disponibles uniquement après leur écriture sur le disque.
- **Écriture différée** : le contrôleur envoie un signal d'achèvement de la requête d'écriture dès que les données sont dans le cache du contrôleur, mais n'ont pas encore été écrites sur le disque. La mise en cache d'écriture différée peut offrir de meilleures performances car les requêtes de lecture suivantes peuvent rapidement récupérer les données sur le cache, puis sur le disque. Cependant, une perte de données peut survenir en cas de défaillance du système, ce qui empêche l'écriture des données sur un disque. D'autres applications peuvent également rencontrer des problèmes lorsque des actions supposent que les données sont disponibles sur le disque.

- **Forcer l'écriture différée** : le cache en écriture est activé, que le contrôleur dispose ou non d'une batterie. Si le contrôleur ne dispose pas d'une batterie et que la mise en mémoire cache d'écriture différée est utilisée, une perte de données peut survenir en cas de coupure d'alimentation.

La règle de mémoire cache de disque s'applique aux lectures sur un disque virtuel spécifique. Ces paramètres n'affectent pas la règle de lecture anticipée.

REMARQUE :

- Le cache non volatile du contrôleur et la sauvegarde par batterie du cache du contrôleur affectent la règle de lecture ou la règle d'écriture qu'un contrôleur peut prendre en charge. Tous les contrôleurs PERC ne possèdent pas de batterie et de cache.
- La lecture anticipée et l'écriture différée nécessitent un cache. Par conséquent, si le contrôleur ne possède pas de cache, il ne vous permet pas de définir la valeur de la règle.
  - De même, si le PERC possède un cache mais pas de batterie et que la règle qui exige l'accès au cache est définie, une perte de données peut se produire en cas de mise hors tension de base. Par conséquent, certains contrôleurs PERC peuvent ne pas autoriser cette règle.
  - Par conséquent, selon le contrôleur PERC, la valeur de la règle est définie.

Suppression de disques virtuels

La suppression d'un disque virtuel détruit toutes les informations, y compris les systèmes de fichiers et les volumes sur le disque virtuel, et supprime le disque virtuel de la configuration du contrôleur. Lors de la suppression de disques virtuels, l'affectation de tous les disques de secours globaux affectés peut être automatiquement annulée lorsque le dernier disque virtuel associé au contrôleur est supprimé. Lors de la suppression du dernier disque virtuel d'un groupe de disques, tous les disques de secours dédiés attribués deviennent automatiquement des disques de secours globaux.

Si vous supprimez tous les disques virtuels d'un disque de secours global, celui-ci est automatiquement supprimé.

Vous devez disposer des privilèges de contrôle du serveur et d'ouverture de session pour procéder à la suppression des disques virtuels.

Lorsque cette opération est autorisée, vous pouvez supprimer un disque virtuel de démarrage. Cette action est effectuée à partir de la bande latérale et indépendamment du système d'exploitation. Par conséquent, un message d'avertissement s'affiche avant la suppression du disque virtuel.

Si vous supprimez un disque virtuel et que vous créez immédiatement un autre disque virtuel ayant les mêmes caractéristiques que celui qui a été supprimé, le contrôleur reconnaît les données comme si le premier disque virtuel n'avait pas été supprimé. Dans ce cas, si vous ne voulez pas conserver les anciennes données après avoir recréé un disque virtuel, réinitialisez le disque virtuel.

REMARQUE : Les opérations de réinitialisation de la configuration et de suppression de disques virtuels ne peuvent pas être empilées avec un maximum de 240 opérations de création de disques virtuels. Cela entraîne l'échec de l'opération. Ces deux opérations peuvent être exécutées sous forme de tâches distinctes avec un intervalle minimum de 2 minutes.

Vérification de cohérence de disque virtuel

Cette opération vérifie l'exactitude des informations (de parité) redondantes. Cette tâche s'applique uniquement aux disques virtuels redondants. Le cas échéant, la tâche de vérification de la cohérence reconstruit les données redondantes. Si le disque virtuel est à l'état Dégradé, il est possible de le faire revenir à l'état Prêt en exécutant une vérification de la cohérence. Vous pouvez effectuer une vérification de la cohérence à l'aide de l'interface Web ou de RACADM.

Vous pouvez également annuler l'opération de vérification de la cohérence. L'annulation de la vérification de cohérence est une opération en temps réel.

Vous devez disposer du privilège de connexion et de contrôle du serveur pour vérifier la cohérence des disques virtuels.

REMARQUE : La vérification de la cohérence n'est pas prise en charge lorsque les disques sont configurés en mode RAID0.

REMARQUE : Si vous effectuez une opération d'annulation de la cohérence alors qu'aucune opération de vérification de cohérence n'est en cours, l'opération en attente dans l'interface GUI s'affiche sous la forme « Annuler l'initialisation en arrière-plan » au lieu de « Annuler la vérification de cohérence ».

Initialisation des disques virtuels

L'initialisation des disques virtuels efface toutes les données du disque, mais ne modifie pas la configuration du disque virtuel. Vous devez initialiser un disque virtuel configuré avant de l'utiliser.

REMARQUE : N'initialisez pas les disques virtuels si vous tentez de recréer une configuration existante.

Vous avez le choix entre l'initialisation rapide, l'initialisation complète ou l'annulation de l'opération d'initialisation.

REMARQUE : L'annulation de l'initialisation est une opération en temps réel. Vous pouvez annuler l'initialisation à l'aide de l'interface Web de l'iDRAC uniquement et non de l'interface RACADM.

Initialisation rapide

L'opération d'initialisation rapide initialise tous les disques physiques inclus dans le disque virtuel. Elle met à jour les métadonnées sur les disques physiques de manière à ce que l'intégralité de l'espace disque soit disponible pour les prochaines opérations d'écriture. Même si les prochaines opérations d'écriture écrasent les informations restantes sur les disques physiques, la tâche d'initialisation peut se terminer rapidement, car les informations existantes sur les disques physiques ne sont pas effacées.

L'initialisation rapide supprime uniquement les informations de répartition et de secteur de démarrage. N'effectuez une initialisation rapide que si vous êtes limité par le temps ou si les disques durs sont neufs ou inutilisés. L'initialisation rapide prend moins de temps (généralement de 30 à 60 secondes).

PRÉCAUTION : L'exécution d'une initialisation rapide rend les données existantes inaccessibles.

La tâche d'initialisation rapide n'écrit pas de zéros sur les blocs de disques des disques physiques. En effet, la tâche d'initialisation rapide n'effectue pas d'opération d'écriture, ce qui réduit la dégradation sur le disque.

Une initialisation rapide sur un disque virtuel écrase les premiers et les derniers 8 Mo du disque virtuel, effaçant ainsi les enregistrements de démarrage ou les informations de partition. L'opération ne prend que 2–3 secondes et est recommandée lorsque vous recréez des disques virtuels.

Une initialisation en arrière-plan démarre cinq minutes après la fin de l'initialisation rapide.

Initialisation complète ou lente

L'opération d'initialisation complète (également appelée initialisation lente) initialise tous les disques physiques inclus dans le disque virtuel. Elle met à jour les métadonnées sur les disques physiques et efface toutes les données et tous les systèmes de fichiers existants. Vous pouvez effectuer une initialisation complète après la création du disque virtuel. Par comparaison avec l'opération d'initialisation rapide, vous pouvez utiliser l'initialisation complète si vous avez des problèmes avec un disque physique ou soupçonnez qu'il contient des blocs de disques endommagés. L'opération d'initialisation complète remappe les blocs endommagés et écrit des zéros sur tous les blocs de disques.

Si vous procédez à l'initialisation complète d'un disque virtuel, l'initialisation en arrière-plan n'est pas nécessaire. Pendant l'initialisation complète, l'hôte ne pourra pas accéder au disque virtuel. Si vous redémarrez le système pendant une initialisation complète, l'opération se termine et une initialisation en arrière-plan démarre sur le disque virtuel.

Il est recommandé de toujours effectuer une initialisation complète sur les disques qui contenaient auparavant des données. L'initialisation complète peut prendre de 1 à 2 minutes par Go. La vitesse d'initialisation dépend du modèle de contrôleur, de la vitesse des disques durs et de la version du firmware.

L'initialisation complète initialise un disque physique à la fois.

REMARQUE : L'initialisation complète est prise en charge uniquement en temps réel. Seuls quelques contrôleurs prennent en charge l'initialisation complète.

Chiffrement de disques virtuels

Lorsque le chiffrement est désactivé sur un contrôleur (autrement dit, la clé de sécurité est supprimée), activez manuellement le chiffrement pour les disques virtuels créés à l'aide de disques SED. Si le disque virtuel est créé après l'activation du chiffrement sur un contrôleur, il est automatiquement chiffré. Il est automatiquement configuré en tant que disque virtuel chiffré, sauf si l'option de chiffrement est désactivée lors de la création du disque virtuel.

Vous devez disposer du privilège de connexion et de contrôle du serveur pour gérer les clés de chiffrement.

REMARQUE : Bien que le chiffrement soit activé dans les contrôleurs, l'utilisateur doit activer manuellement le chiffrement sur le disque virtuel si ce dernier est créé à partir de l'iDRAC.

Affectation ou annulation de l'affectation de disques de secours dédiés

Un disque de secours dédié est un disque de sauvegarde inutilisé attribué à un disque virtuel. Lorsqu'un disque physique du disque virtuel échoue, le disque de secours est activé pour remplacer le disque physique problématique sans que le système ne soit interrompu ou que votre intervention ne soit requise

Vous devez disposer des privilèges de contrôle du serveur et d'ouverture de session pour exécuter cette opération.

Vous pouvez affecter uniquement des disques 4K en tant que disques de secours à des disques virtuels 4K.

Si vous avez affecté un disque physique en tant que disque de secours dédié en mode Ajouter à l'opération en attente, l'opération en attente est créée, mais pas la tâche. Si vous tentez ensuite d'annuler l'affectation du disque de secours dédié, l'opération en attente d'affectation de disque de secours dédié est désactivée.

Si vous avez annulé l'affectation d'un disque physique en tant que disque de secours dédié en mode Ajouter à l'opération en attente, l'opération en attente est créée, mais pas la tâche. Si vous tentez ensuite d'affecter le disque de secours dédié, l'opération en attente d'annulation d'affectation de disque de secours dédié est désactivée.

REMARQUE : Lorsque l'opération d'exportation du journal est en cours, vous ne pouvez pas afficher d'informations sur les disques de secours dédiés sur la page **Gérer les disques virtuels**. Une fois l'opération d'exportation du journal terminée, rechargez ou actualisez la page **Gérer les disques virtuels** pour afficher les informations.

Renommer disque virtuel

Pour modifier le nom d'un disque virtuel, l'utilisateur doit disposer du privilège de Contrôle du système. Le nom du disque virtuel ne peut contenir que des caractères alphanumériques, des tirets et des traits de soulignement. La longueur maximale du nom dépend de chaque contrôleur. Dans la plupart des cas, la longueur maximale est de 15 caractères. Chaque fois qu'un disque virtuel est renommé, un journal LC est créé.

Modifier la volumétrie

L'extension de capacité en ligne (OCE) vous permet d'augmenter la capacité de stockage des niveaux de RAID sélectionnés tout en maintenant la connectivité du système. Le contrôleur redistribue les données sur la baie (processus de reconfiguration), en plaçant un nouvel espace disponible à la fin de chaque baie RAID.

L'extension de capacité en ligne (OCE) peut s'effectuer de deux façons :

- Si de l'espace libre est disponible sur le plus petit disque physique du groupe de disques virtuels après le démarrage du LBA des disques virtuels, la capacité du disque virtuel peut être étendue dans cet espace libre. Cette option vous permet d'entrer la nouvelle taille revue à la hausse du disque virtuel. Si de l'espace libre est disponible sur un groupe de disques d'un disque virtuel uniquement avant le démarrage du LBA, alors Modifier Capacité de disque n'est pas autorisé dans le même groupe de disques, même si de l'espace disponible existe sur un disque physique.
- Vous pouvez également étendre la capacité d'un disque virtuel en ajoutant des disques physiques compatibles au groupe de disques virtuels existant. Cette option ne vous permet pas d'entrer la nouvelle taille revue à la hausse du disque virtuel. Cette dernière est calculée et affichée à l'utilisateur en fonction de l'espace disque utilisé par le groupe de disques physiques existant d'un disque virtuel particulier, du niveau de raid existant du disque virtuel et du nombre de nouveaux lecteurs ajoutés au disque virtuel.

L'extension de capacité permet à l'utilisateur de spécifier la taille finale du disque virtuel. En interne, la taille finale du disque virtuel est transmise au contrôleur PERC en pourcentage (ce pourcentage correspond à l'espace que l'utilisateur souhaite utiliser à partir de l'espace vide restant dans la baie pour l'extension du disque local). En raison de cette logique de pourcentage, la taille finale du disque virtuel après la fin de la reconfiguration peut être différente de celle fournie par l'utilisateur dans le cas où l'utilisateur n'attribue pas la taille maximale possible du disque virtuel en tant que taille de disque virtuel finale (le pourcentage s'avère inférieur à 100 %). L'utilisateur ne voit pas de différence entre la taille du disque virtuel saisie et la taille finale du disque virtuel après la reconfiguration, si la taille maximale possible du disque virtuel est saisie par l'utilisateur.

Migration du niveau de RAID

La modification du niveau RAID d'un disque virtuel est appelée RAID-Level migration (RLM). L'iDRAC fournit une option permettant d'augmenter la taille du disque virtuel à l'aide de RLM. Dans un sens, RLM permet la migration du niveau de RAID d'un disque virtuel qui à son tour peut augmenter la taille des disques virtuels.

La migration du niveau de RAID est le processus de conversion d'un disque virtuel avec un niveau de RAID à un autre. Lors de la migration d'un disque virtuel vers un autre niveau de RAID, les données utilisateur sur celui-ci sont réparties sur le format de la nouvelle configuration.

Cette configuration est prise en charge par les états préparés et en temps réel.

Le tableau suivant décrit ci-dessous les dispositions de reconfiguration possible du disque virtuel en reconfigurant un disque virtuel (RLM) avec un ajout de disques et sans ajout de disques.

Tableau 46. Dispositions de disque virtuel possible

Disposition de disque virtuel source	Disposition de disque virtuel cible possible avec un ajout de disques	Disposition de disque virtuel cible possible sans ajout de disques
R0 (disque unique)	R1	S/O
R0	R5/R6	S/O
R1	R0/R5/R6	R0
Par R5	R0/R6	R0
Par R6	R0/R5	R0/R5

Opérations autorisées lorsque OCE ou RLM s'active

Les opérations suivantes sont autorisées quand RLM/OCE est en cours :

Tableau 47. Opérations autorisées

À partir de l'extrémité du contrôleur derrière lequel un disque virtuel passe par RLM/OCE	À partir de l'extrémité du disque virtuel (qui passer par l'OCE/RLM)	À partir de tout autre disque physique en état Prêt sur le même contrôleur	À partir de toute autre extrémité de disque virtuel (qui ne passe par l'OCE/ RLM) sur le même contrôleur
Redéfinir la configuration	Supprimer	Faire clignoter	Supprimer
Journal d'exportation	Faire clignoter	Arrêter le clignotement	Faire clignoter
Définir le mode de lecture cohérente	Arrêter le clignotement	Attribuer le disque de secours global	Arrêter le clignotement
Démarrer la lecture cohérente	S/O	Convertir en disques non-RAID	Renommer
Modifier les propriétés du contrôleur	S/O	S/O	Changer de règle
Gérer l'alimentation du disque physique	S/O	S/O	Initialisation lente
Convertir en disques de RAID aptes	S/O	S/O	Initialisation rapide
Convertir en disques non-RAID	S/O	S/O	Remplacer un disque membre
Modifier le mode du contrôleur	S/O	S/O	S/O

Annuler l'initialisation

Cette fonctionnalité permet d'annuler l'initialisation en arrière-plan sur un disque virtuel. Sur les contrôleurs PERC, l'initialisation en arrière-plan du disque virtuel redondant démarre automatiquement après la création du disque virtuel. L'initialisation en arrière-plan du disque virtuel redondant prépare le disque virtuel pour vérifier les informations de parité et améliore les performances en écriture. Il est cependant impossible d'exécuter certains processus tels que la création d'un disque virtuel durant l'initialisation en arrière-plan. L'option

Annuler l'initialisation permet d'annuler manuellement l'initialisation en arrière-plan. Une fois annulée, l'initialisation en arrière-plan est automatiquement relancée dans un délai de 0 à 5 minutes.

REMARQUE : L'initialisation en arrière-plan est impossible sur les disques virtuels RAID 0.

Restrictions ou limitations relatives à l'extension de capacité en ligne (OCE) et à la migration de niveau de RAID (RLM)

Les principales limitations relatives à l'OCE et à la RLM sont les suivantes :

- L'OCE et la RLM sont limitées aux scénarios dans lesquels le groupe de disques ne contient qu'un seul disque virtuel.
- L'OCE n'est pas prise en charge sur les niveaux RAID50 et RAID60. La RLM n'est pas prise en charge sur les niveaux RAID10, RAID50 et RAID60.
- Si le contrôleur contient déjà le nombre maximal de disques virtuels, vous ne pouvez pas effectuer de migration du niveau RAID ou d'extension de capacité sur aucun disque virtuel.
- Le contrôleur convertit la stratégie du cache en écriture de tous les disques virtuels impliqués dans l'opération d'extension de capacité en ligne (OCE)/de migration de niveau de RAID (RLM) en mode d'écriture immédiate jusqu'à ce que l'opération soit terminée.
- La reconfiguration de disques virtuels affecte habituellement les performances des disques tant que l'opération de reconfiguration n'est pas terminée.
- Un groupe de disques ne peut pas contenir plus de 32 disques physiques.
- Si une opération en arrière-plan (par exemple, initialisation en arrière-plan/reconstruction/recopie/lecture cohérente) est en cours d'exécution sur le disque virtuel ou le disque physique correspondant, la reconfiguration (OCE/RLM) n'est pas autorisée à ce moment-là.
- Tout type de migration de disque lorsque la reconfiguration (OCE/RLM) est en cours sur les disques associés au disque virtuel entraîne l'échec de la reconfiguration.
- Tout nouveau disque ajouté pour l'OCE/la RLM devient une partie du disque virtuel à la fin de la reconstruction. Néanmoins, ces nouveaux disques passent à l'état En ligne juste après le début de la reconstruction.

Gestion de disques virtuels à l'aide de RACADM

Utilisez les commandes suivantes pour gérer les disques virtuels :

- Pour supprimer un disque virtuel :

```
racadm storage deletevd:<VD FQDD>
```

- Pour initialiser un disque virtuel :

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

- Pour vérifier la cohérence des disques virtuels (non pris en charge sur RAID0) :

```
racadm storage ccheck:<vdisk fqdd>
```

  Pour annuler une vérification de cohérence :

```
racadm storage cancelcheck: <vdisks fqdd>
```

- Pour chiffrer des disques virtuels :

```
racadm storage encryptvd:<VD FQDD>
```

- Pour affecter des disques de secours dédiés ou annuler leur affectation :

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of VD>
```

<option>=yes

Attribuer un disque de secours

<Option>=no

Annuler l'attribution d'un disque de secours

Gestion de disques virtuels à l'aide de l'interface web

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Disques virtuels**.
2. À partir de **Disques virtuels**, sélectionnez le contrôleur dont vous souhaitez gérer les disques virtuels.
3. Sélectionnez une action à partir du menu déroulant **Action**.

   Lorsque vous sélectionnez une action, une fenêtre **Action** supplémentaire s'affiche. Sélectionnez/saisissez la valeur souhaitée.
   - **Renommer**
   - **Supprimer**
   - **Modifier la règle de mise en cache** : vous permet de modifier la règle de mise en cache pour les options suivantes :
     - **Règle de lecture** : les valeurs suivantes peuvent être sélectionnées :
       - **Lecture anticipée adaptative** : indique que, pour le volume donné, la commande utilise la règle de mémoire cache Lecture vers l'avant si les deux accès les plus récents aux disques se sont produits dans des secteurs séquentiels. Si les demandes de lecture sont aléatoires, le contrôleur revient au mode Pas de lecture anticipée.
       - **Pas de lecture anticipée** : indique que pour le volume donné, aucune règle de lecture anticipée n'est utilisée.
       - **Lecture anticipée** : indique que pour le volume donné, le contrôleur lit de manière séquentielle vers l'avant des données demandées et stocke les données supplémentaires dans la mémoire cache, anticipant une exigence de données. Cela accélère les lectures de données séquentielles, mais l'amélioration est moindre lors de l'accès aux données aléatoires.
     - **Règle en écriture** : permet de choisir l'une des règles de cache en écriture suivantes :
       - **Écriture immédiate** : indique que pour le volume donné, le contrôleur envoie un signal d'achèvement du transfert de données au système hôte lorsque le sous-système du disque a reçu toutes les données d'une transaction.
       - **Écriture différée** : indique que pour le volume donné, le contrôleur envoie un signal d'achèvement du transfert de données au système hôte une fois que la mémoire cache du contrôleur a reçu toutes les données d'une transaction. Le contrôleur écrit ensuite les données placées en mémoire cache dans l'appareil de stockage à l'arrière-plan.
       - **Forcer l'écriture différée** : lors de l'utilisation de l'option forcer la mise en mémoire cache en écriture différée, la mémoire cache en écriture est activée, que le contrôleur dispose ou non d'une batterie. Si le contrôleur ne dispose pas d'une batterie et que la mise en mémoire cache d'écriture différée est utilisée, une perte de données peut survenir en cas de coupure d'alimentation.
     - **Règle de cache de disque** : permet de choisir l'une des règles de cache de disque suivantes :
       - **Par défaut** : indique que le disque utilise son mode de mémoire cache en écriture par défaut. Pour les disques SATA, cette option est activée et pour les disques SAS, elle est désactivée.
       - **Activée** : indique que la mémoire cache en écriture du disque est activée. Cela améliore les performances et la probabilité de perte de données en cas de panne d'alimentation.
       - **Désactivée** : indique que la mémoire cache en écriture du disque est désactivée. Cela réduit les performances et la probabilité de perte de données.
   - **Modifier la volumétrie du disque** : vous pouvez ajouter les disques physiques au disque virtuel sélectionné dans cette fenêtre. Cette fenêtre affiche également la capacité actuelle et la nouvelle capacité du disque virtuel après l'ajout de disques physiques.
   - **Migration de niveau de RAID** : affiche le nom du disque, le niveau de RAID actuel et la taille du disque virtuel. Permet de sélectionner un nouveau niveau de RAID. Il est possible que l'utilisateur doive ajouter d'autres lecteurs aux disques virtuels existants pour migrer vers un nouveau niveau de raid. Cette fonction ne s'applique pas à RAID 10, 50 et 60.
   - **Initialisation : rapide** : met à jour les métadonnées sur les disques physiques de manière à ce que tout l'espace disque soit disponible pour les prochaines opérations d'écriture. Même si les prochaines opérations d'écriture écrasent les informations restantes sur les disques physiques, l'option initialiser peut être terminée rapidement car les informations existantes sur les disques physiques ne sont pas effacées.
   - **Initialisation : complète** : toutes les données et tous les systèmes de fichiers existants sont supprimés.

     REMARQUE : L'option **Initialiser : plein** ne s'applique pas aux contrôleurs PERC H330.

   - **Vérification de la cohérence** – Pour contrôler la cohérence d'un disque virtuel, sélectionnez **Vérifier la cohérence** dans le menu déroulant correspondant.

     REMARQUE : La vérification de la cohérence n'est pas prise en charge sur des disques configurés en mode RAID0.

   Pour plus d'informations sur ces options, voir l'**aide en ligne d'iDRAC**.
4. Cliquez sur **Appliquer maintenant** pour appliquer les modifications immédiatement, sur **Au prochain redémarrage** pour appliquer les modifications après le prochain redémarrage, sur **À l'heure planifiée** pour appliquer les modifications à une heure donnée, et sur **Annuler toutes les opérations en attente** pour annuler les modifications.

   Les paramètres sont appliqués en fonction du mode de fonctionnement sélectionné.

Fonctionnalités de configuration RAID

Le tableau suivant répertorie certaines des fonctionnalités de configuration RAID qui sont disponibles dans RACADM :

PRÉCAUTION : Le forçage d'un disque physique pour le mettre en ligne ou hors ligne peut provoquer une perte de données.

Tableau 48. Fonctionnalités de configuration RAID

Fonctionnalité	Commande RACADM	Description
Mise en ligne forcée	`racadm storage forceonline:<PD FQDD>`	Une coupure d'alimentation, des données corrompues, ou une autre raison peut conduire un disque physique à passer hors ligne. Vous pouvez utiliser cette fonctionnalité pour forcer un disque physique à se remettre à l'état En ligne lorsque toutes les autres options sont épuisées. Une fois que la commande est exécutée, le contrôleur remet le lecteur à l'état En ligne et restaure ses membres au sein du disque virtuel. Cela se produit uniquement si le contrôleur peut lire les données du lecteur et peut écrire dans ses métadonnées.
REMARQUE : La récupération de données n'est possible que si une petite portion du disque est endommagée. La fonctionnalité Forcer en ligne ne peut pas corriger un disque déjà défectueux.		
Mise hors ligne forcée	`racadm storage forceoffline:<PD FQDD>`	Cette fonctionnalité supprime un lecteur d'une configuration de disque virtuel afin que celui-ci passe hors ligne, ce qui pourrait causer une configuration de disque virtuel dégradé. C'est utile si un lecteur est susceptible de tomber en panne dans un futur proche ou signale une panne SMART mais qu'il est toujours en ligne. Cette fonctionnalité peut être également utilisée si vous souhaitez utiliser un lecteur qui fait partie d'une configuration RAID existante.
Remplacement du disque physique	`racadm storage replacephysicaldisk:<Source PD FQDD > -dstpd <Destination PD FQDD>`	Vous permet de copier des données à partir d'un disque physique qui est membre d'un disque virtuel, sur un autre disque physique. Le disque source doit être à l'état En ligne, alors que le disque de destination doit être à l'état Prêt et de même taille et type pour remplacer le disque source.
Disque virtuel en tant que périphérique de démarrage	`racadm storage setbootvd:<controller FQDD> -vd <VirtualDisk FQDD>`	Un disque virtuel peut être configuré comme un périphérique de démarrage à l'aide de cette fonctionnalité. Cela permet la tolérance de pannes lorsqu'un disque virtuel avec redondance est sélectionné en tant que périphérique de démarrage, et sur lequel le système d'exploitation est installé.
Déverrouillage d'une configuration étrangère	`racadm storage unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>`	Cette fonctionnalité est utilisée pour authentifier les lecteurs verrouillés qui ont un chiffrement du contrôleur source différent du disque de destination. Une fois déverrouillé, le lecteur peut être migré d'un contrôleur vers un autre.

Gestion des contrôleurs

Vous pouvez effectuer les tâches suivantes pour les contrôleurs :

- Configurer les propriétés du contrôleur
- Importer ou importer automatiquement une configuration étrangère
- Effacer la configuration étrangère
- Réinitialiser la configuration d'un contrôleur
- Créer, modifier ou supprimer des clés de sécurité
- Suppression du cache conservé

Configuration des propriétés du contrôleur

Vous pouvez configurer les propriétés suivantes du contrôleur :

- Mode de lecture cohérente (automatique ou manuelle)
- Démarrer ou arrêter la lecture cohérente si le mode de lecture cohérente est Manuel
- Zones non configurées de la lecture cohérente
- Mode de vérification de la cohérence
- Mode de recopie
- Mode d'équilibrage de charge
- Taux de vérification de la cohérence
- Taux de recréation
- Taux d'initialisation en arrière-plan (BGI)
- Taux de reconstruction
- Configuration étrangère d'importation automatique optimisée
- Créez ou modifiez les clés de sécurité
- Mode de chiffrement (Gestion des clés locale et Secure Enterprise key Manager)

Vous devez disposer du privilège de connexion et de contrôle du serveur pour configurer les propriétés du contrôleur.

Remarques sur le mode de lecture cohérente

La lecture cohérente identifie les erreurs de disque pour éviter les pannes de disque, ainsi que la perte ou la corruption de données. Il s'exécute automatiquement une fois par semaine sur les disques durs SAS et SATA.

La lecture cohérente n'est pas exécutée sur un disque physique dans les cas suivants :

- Le disque physique est du type SSD.
- Le disque physique ne fait pas partie d'un disque virtuel ou n'est pas attribué comme disque de secours.
- Le disque physique fait partie d'un disque virtuel qui fait actuellement l'objet d'une des tâches suivantes :
  - Une recréation
  - Une reconfiguration ou une reconstruction
  - Une initialisation en arrière-plan
  - Une vérification de cohérence

De plus, la lecture cohérente s'interrompt pendant une activité d'E/S importante et reprend lorsque l'activité d'E/S est terminée.

REMARQUE : Consultez la documentation du contrôleur pour plus d'informations sur la fréquence d'exécution de la tâche de lecture cohérente lorsqu'elle est en mode automatique.

REMARQUE : Les opérations en mode Lecture cohérente telles que **Démarrer** et **Arrêter** ne sont pas prises en charge en l'absence de disques virtuels disponibles dans le contrôleur. Vous pouvez appeler les opérations en utilisant les interfaces iDRAC, mais les opérations échouent lors du démarrage de la tâche correspondante.

Équilibrage de charge

La propriété Équilibrage des charges permet d'utiliser automatiquement les ports ou les connecteurs du contrôleur raccordés au même boîtier pour acheminer les requêtes d'E/S. Cette propriété est disponible uniquement pour les contrôleurs SAS.

Taux d'initialisation en arrière-plan (BGI)

Sur les contrôleurs PERC, l'initialisation en arrière-plan d'un disque virtuel redondant débute automatiquement dans un délai de 0 à 5 minutes après la création du disque virtuel. L'initialisation en arrière-plan d'un disque virtuel redondant prépare le disque virtuel pour assurer la redondance des données et améliorer les performances en écriture. Par exemple, lors de l'initialisation d'un disque virtuel RAID 5 effectuée en arrière-plan, les informations de parité sont initialisées. Lors de l'initialisation d'un disque virtuel RAID 1 en arrière-plan, les disques physiques sont mis en miroir.

L'initialisation en arrière-plan permet au contrôleur d'identifier et de corriger les éventuels problèmes ultérieurs liés aux données redondantes. De ce point de vue, l'initialisation en arrière-plan est similaire à la vérification de la cohérence. Il est recommandé de permettre l'exécution de l'initialisation en arrière-plan. Si vous l'annulez, l'initialisation en arrière-plan est automatiquement relancée dans un délai de 0 à 5 minutes. Certains processus peuvent être exécutés durant l'initialisation en arrière-plan, notamment les opérations de lecture et d'écriture. D'autres processus tels que la création d'un disque virtuel ne peuvent pas être exécutés durant l'initialisation en arrière-plan. Ces processus entraînent l'annulation de l'initialisation en arrière-plan.

Le taux de l'initialisation en arrière-plan (configurable entre 0 et 100 %) représente le pourcentage des ressources système dédiées à l'exécution de la tâche d'initialisation en arrière-plan. À un taux de 0 %, la priorité de l'initialisation en arrière-plan est la plus faible pour le contrôleur, son exécution est très lente et son impact sur les performances du système le plus faible possible. Une initialisation en arrière-plan d'un taux de 0 % ne signifie pas que le processus est arrêté ou interrompu. À un taux de 100 %, l'initialisation en arrière-plan a la priorité la plus élevée pour le contrôleur. L'exécution de l'initialisation est très rapide et son impact sur les performances du système est le plus élevé.

Vérifier la cohérence

La vérification de la cohérence vérifie l'exactitude des informations (de parité) redondantes. Cette tâche s'applique uniquement aux disques virtuels redondants. Le cas échéant, l'opération de vérification de la cohérence reconstruit les données redondantes. Lorsqu'un disque virtuel est à l'état Défaillance de la redondance, l'exécution de la vérification de cohérence peut permettre de rétablir l'état Prêt du disque virtuel.

Le taux de la vérification de la cohérence (configurable entre 0 et 100 %) représente le pourcentage des ressources système dédiées à l'exécution de la vérification de la cohérence. À un taux de 0 %, la priorité de la vérification de la cohérence est la plus faible pour le contrôleur, son exécution est très lente et son impact sur les performances du système est la plus faible possible. Lorsque le taux de la vérification de la cohérence est de 0 %, cela ne signifie pas que le processus est arrêté ou interrompu. À un taux de 100 %, la vérification de la cohérence en arrière-plan a la priorité la plus élevée pour le contrôleur. L'exécution de la vérification de la cohérence sera très rapide et aura l'impact le plus élevé sur les performances du système.

Configuration des propriétés des contrôleurs à l'aide de RACADM

- Pour définir le mode de lecture cohérente :

```
racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
```

- Si le mode de lecture cohérente est défini sur Manuel, utilisez les commandes suivantes pour démarrer et arrêter le mode Lecture cohérente :

```
racadm storage patrolread:<Controller FQDD> -state {start|stop}
```

REMARQUE : Les opérations en mode Lecture cohérente telles que Démarrer et Arrêter ne sont pas prises en charge en l'absence de disques virtuels disponibles dans le contrôleur. Vous pouvez appeler les opérations en utilisant l'interface de l'iDRAC, mais les opérations échouent lors du démarrage de la tâche correspondante.

REMARQUE : Les attributs de stockage PatrolReadMode et PersistHotSpare, qui sont assignés aux contrôleurs HBA12 et PERC12, ne sont pas modifiables. Si vous tentez de modifier ces attributs, vous risquez de rencontrer des erreurs. Bien que le travail soit créé et exécuté, les valeurs d'origine restent les mêmes.

- Pour spécifier le mode de Vérification de cohérence, utilisez l'objet **Storage.Controller.CheckConsistencyMode**.
- Pour activer ou désactiver le mode de Recopie, utilisez l'objet **Storage.Controller.CopybackMode**.
- Pour activer ou désactiver le mode d'équilibrage de charge, utilisez l'objet **Storage.Controller.PossibleloadBalancedMode**.
- Pour spécifier le pourcentage de ressources système dédiées à l'exécution d'une vérification de cohérence sur un disque virtuel redondant, utilisez l'objet **Storage.Controller.CheckConsistencyRate**.

- Pour spécifier le pourcentage de ressources du contrôleur dédiées à la reconstruction d'un disque en échec, utilisez l'objet **Storage.Controller.RebuildRate**
- Pour spécifier le pourcentage de ressources du contrôleur dédiées à l'exécution de l'initialisation en arrière-plan (BGI) d'un disque virtuel après sa création, utilisez l'objet **Storage.Controller.BackgroundInitializationRate**.
- Pour spécifier le pourcentage de ressources du contrôleur dédiées à la reconstruction d'un groupe de disques après l'ajout d'un disque physique ou la modification du niveau de RAID d'un disque virtuel résidant sur le groupe de disques, utilisez l'objet **Storage.Controller.ReconstructRate**
- Pour activer ou désactiver l'importation automatique optimisée d'une configuration étrangère pour le contrôleur, utilisez l'objet **Storage.Controller.EnhancedAutoImportForeignConfig**
- Pour créer, modifier ou supprimer la clé de sécurité pour chiffrer les disques virtuels :

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd <passphrase>
racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd <old
passphrase> -newpasswd <new passphrase>
racadm storage deletesecuritykey:<Controller FQDD>
```

Configuration des propriétés des contrôleurs à l'aide de l'interface Web

1. Dans l'interface Web iDRAC, accédez à **Stockage** > **Présentation** > **Contrôleurs**.
   La page **Configurer les contrôleurs** s'affiche.
2. Dans la section **Contrôleur**, sélectionnez le contrôleur que vous souhaitez configurer.
3. Spécifiez les informations requises pour les différentes propriétés.

   La colonne **Valeur actuelle** affiche la valeur existante de chaque propriété. Vous pouvez modifier cette valeur en sélectionnant l'option adéquate dans le menu déroulant **Action** de chaque propriété.

   Pour plus d'informations sur les champs, voir l'**Aide en ligne d'iDRAC**.
4. Dans **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez appliquer les paramètres.
5. Cliquez sur **Appliquer**.

   Les paramètres sont appliqués en fonction du mode de fonctionnement sélectionné.

Security Protocol and Data Model (SPDM)

Le protocole SPDM est utilisé pour établir l'authenticité et les fonctionnalités de sécurité entre les composants matériels. SPDM permet l'échange de messages entre l'iDRAC et les appareils distants tels que les contrôleurs de stockage (PERC12), FC et CPU. Cela inclut les certificats d'identité du matériel. Vous pouvez activer SPDM à l'aide de Redfish ou RACADM.

Tableau 49. Licences pour fonctionnalités SPDM

Fonctionnalité	Licence
Inventaire - Détection des appareils prenant en charge SPDM	Pas sous licence
Collecte de l'identité matérielle des appareils	Enterprise
Collecte des mesures des appareils	Enterprise
Établissement d'un certificat d'appareil de confiance à l'aide de SCV	Licence SCV
Canal de communication chiffré	Licence SEKM

Lorsqu'un appareil est pris en charge par SPDM, les données SCV collectées contiennent des certificats d'identité du matériel SPDM en plus des champs existants. Les certificats d'identité du firmware ne sont pas dans le certificat SCV.

REMARQUE : Vous pouvez remarquer que le numéro de port de la carte NIC est absent du nom du fichier de certificat du matériel SPDM téléchargé.

REMARQUE : L'échec de la tâche d'exportation du certificat SPDM est affiché dans la file d'attente des tâches lorsque vous exécutez des redémarrages fréquents.

Activer SPDM à l'aide de RACADM

La fonctionnalité SPDM de l'iDRAC vous permet de gérer et de surveiller l'état de sécurité de divers composants.

1. Exécutez la commande suivante pour activer SPDM :
   ```
   racadm set idrac.SPDM.enable enabled
   ```
2. Exécutez les commandes suivantes pour vous assurer que les modifications sont reflétées :
   ```
   racadm racreset
   racadm get idrac.SPDM
   ```

Activer SPDM à l'aide de Redfish

La fonctionnalité SPDM de l'iDRAC vous permet de gérer et de surveiller l'état de sécurité de divers composants.

1. Exécutez une demande de CORRECTIF pour l'URI suivant à l'aide de la charge utile `{"Attributes": {"SPDM.1.Enable":"Enabled"}}` :
   ```
   /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1
   ```
2. Exécutez `racreset` pour vous assurer que les modifications sont reflétées.

Importation ou importation automatique d'une configuration étrangère

Une configuration étrangère est composée de données se trouvant sur des disques physiques qui ont été déplacées d'un contrôleur à un autre. Les disques virtuels résidant sur des disques physiques qui ont été déplacés sont considérés comme une configuration étrangère.

Vous pouvez importer des configurations étrangères pour éviter la perte de disques virtuels suite au déplacement des disques physiques. Une configuration étrangère peut être importée uniquement si elle contient un disque virtuel dont l'état est défini sur Prêt ou Dégradé ou un disque de secours dédié à un disque virtuel qui peut être importé ou qui est déjà présent.

Toutes les données du disque virtuel doivent être présentes, mais si le disque virtuel utilise un niveau de RAID redondant, les données redondantes supplémentaires ne sont pas requises.

Par exemple, si la configuration étrangère ne contient qu'un seul côté d'un miroir dans un disque virtuel RAID 1, le disque virtuel est à l'état dégradé et peut être importé. Si la configuration étrangère ne contient qu'un seul disque physique qui a été initialement configuré en tant que RAID 5 à l'aide de trois disques physiques, le disque virtuel RAID 5 est à l'état Échec et ne peut pas être importé.

Outre les disques virtuels, une configuration étrangère peut être composée d'un disque physique qui a été affecté en tant que disque de secours d'un contrôleur puis déplacé vers un autre contrôleur. La tâche Importer la configuration étrangère importe le nouveau disque physique en tant que disque de secours. Si le disque physique a été défini en tant que disque de secours dédié sur la version précédente du contrôleur, mais que le disque virtuel auquel le disque de secours a été attribué n'est plus présent dans la configuration étrangère, le disque physique est importé en tant que disque de secours global.

La tâche Importer la configuration étrangère s'affiche uniquement lorsque le contrôleur a détecté une configuration étrangère. Vous pouvez également identifier si un disque physique contient une configuration étrangère (disque virtuel ou disque de secours) par la vérification de l'état du disque physique. Si l'état du disque physique est Étranger, le disque physique contient tout ou une partie d'un disque virtuel, ou un disque de secours lui est attribué.

REMARQUE : Dans le cadre de l'importation d'une configuration étrangère, si une configuration est incomplète, elle n'est pas importée. Néanmoins, la tâche n'échouera pas. L'état de la tâche s'affiche comme **Terminé avec succès**. Vous devez vérifier l'état du disque physique pour savoir si le disque virtuel est importé ou non.

REMARQUE : La tâche d'importation d'une configuration étrangère importe tous les disques virtuels résidant sur des disques physiques qui ont été ajoutés au contrôleur. Si plusieurs disques virtuels étrangers sont présents, toutes les configurations étrangères sont importées.

Le contrôleur PERC9 prend en charge l'importation automatique d'une configuration étrangère sans interaction de l'utilisateur. L'importation automatique peut être activée ou désactivée. En cas d'activation, le contrôleur PERC peut importer automatiquement toute configuration étrangère détectée sans intervention manuelle. En cas de désactivation, le contrôleur PERC n'importe pas automatiquement de configurations étrangères.

Vous devez disposer du privilège de connexion et de contrôle du serveur pour importer des configurations étrangères.

Cette tâche n'est pas prise en charge sur les contrôleurs matériels PERC s'exécutant en mode HBA.

REMARQUE : Il est déconseillé de débrancher un câble d'enceinte externe pendant que le système d'exploitation s'exécute sur le système. Le retrait du câble peut entraîner l'adoption d'une configuration étrangère lorsque la connexion est rétablie.

Vous pouvez gérer les configurations étrangères dans les cas suivants :

- Tous les disques physiques d'une configuration sont retirés et réinstallés.
- Certains des disques physiques d'une configuration sont retirés et réinstallés.
- Tous les disques physiques d'un disque virtuel sont retirés à des moments différents, puis réinstallés.
- Les disques physiques d'un disque virtuel non redondant sont retirés.

Les contraintes suivantes s'appliquent aux disques physiques que vous envisagez d'importer :

- L'état d'un disque physique peut changer entre le moment où la configuration étrangère est analysée et celui où l'importation proprement dite est effectuée. L'importation étrangère ne se produit que sur les disques dont l'état est défini sur Non configuré - Bon.
- Les lecteurs défectueux ou hors ligne ne peuvent pas être importés.
- Le firmware ne vous permet pas d'importer ou d'effacer les configurations étrangères si plus de huit disques étrangers sont présents.

Importation d'une configuration étrangère à l'aide de RACADM

Pour importer la configuration étrangère :

```
racadm storage importconfig:<Controller FQDD>
```

Pour en savoir plus, voir le **Guide de référence de la ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**.

Importation d'une configuration étrangère à l'aide de l'interface Web

REMARQUE : S'il existe une configuration de disque externe incomplète dans le système, l'état du ou des disques virtuels en ligne figure également comme externe.

REMARQUE : L'importation d'une configuration étrangère pour le contrôleur BOSS n'est pas prise en charge.

Pour importer la configuration étrangère :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Contrôleurs**.
2. Dans les options **Contrôleur**, sélectionnez le contrôleur dans lequel vous souhaitez importer la configuration étrangère.
3. Cliquez sur **Importer** sous la **Configuration étrangère**, puis cliquez sur **Appliquer**.

Suppression d'une configuration étrangère

Après avoir déplacé un disque physique d'un contrôleur à l'autre, il se peut que le disque physique contienne la totalité ou une partie d'un disque virtuel (la configuration étrangère). Vous pouvez également identifier si un disque physique précédemment utilisé contient une configuration étrangère (disque virtuel) en vérifiant l'état du disque physique. Si l'état du disque physique est Étranger, le disque physique contient tout ou une partie d'un disque virtuel. Vous pouvez effacer ou supprimer les informations du disque virtuel des disques physiques nouvellement connectés.

L'opération Effacer une configuration étrangère efface définitivement toutes les données se trouvant sur les disques physiques ajoutés au contrôleur. Si plusieurs disques virtuels étrangers sont présents, toutes les configurations sont supprimées. Il est éventuellement préférable d'importer le disque virtuel plutôt que de détruire les données. Une initialisation doit être effectuée pour supprimer les données étrangères. Si vous disposez d'une configuration étrangère incomplète ne pouvant pas être importée, vous pouvez utiliser l'option Suppression d'une configuration étrangère pour effacer les données étrangères présentes sur les disques physiques.

Suppression d'une configuration étrangère à l'aide de l'interface Web

Pour supprimer une configuration étrangère :

1. Dans l'interface Web iDRAC, accédez à **Stockage** > **Présentation** > **Contrôleurs**.
   La page **Configuration du contrôleur** s'affiche.
2. Dans les options **Contrôleur**, sélectionnez le contrôleur dont vous voulez effacer la configuration étrangère.

   REMARQUE : Pour effacer la configuration étrangère des contrôleurs BOSS, cliquez sur **Réinitialiser la configuration**.
3. Cliquez sur **Effacer la configuration**.
4. Cliquez sur **Apply**
   Les disques virtuels qui résident sur le disque physique sont effacés en fonction du mode de fonctionnement sélectionné.

Effacement d'une configuration étrangère à l'aide de RACADM

Pour effacer une configuration étrangère :

```
racadm storage clearconfig:<Controller FQDD>
```

Pour en savoir plus, voir le **Guide de référence de la ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**.

Réinitialisation de la configuration d'un contrôleur

Vous pouvez réinitialiser la configuration d'un contrôleur. Cette opération supprime les lecteurs de disque virtuel et annule l'attribution de tous les disques de secours sur le contrôleur. Elle n'efface aucune donnée autre que le retrait des disques de la configuration. Par ailleurs, la réinitialisation de la configuration ne supprime pas les configurations étrangères. La réinitialisation de la configuration n'efface pas toutes les données. Vous pouvez recréer exactement la même configuration sans opération d'initialisation, qui peut entraîner la récupération des données. Vous devez disposer des privilèges de contrôle du serveur.

REMARQUE : La redéfinition de la configuration du contrôleur ne supprime pas une configuration étrangère. Pour supprimer une configuration étrangère, exécutez une opération d'effacement de la configuration.

Réinitialisation de la configuration d'un contrôleur à l'aide de l'interface Web

Pour redéfinir la configuration du contrôleur :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Contrôleurs**.
2. Dans **Actions**, sélectionnez l'option **Réinitialiser la configuration** en regard d'un ou de plusieurs contrôleurs.
3. Pour chaque contrôleur, dans le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez appliquer les paramètres.
4. Cliquez sur **Appliquer**.

   Les paramètres sont appliqués en fonction du mode de fonctionnement sélectionné.

Réinitialisation de la configuration d'un contrôleur à l'aide de RACADM

Pour redéfinir la configuration du contrôleur :

```
racadm storage resetconfig:<Controller FQDD>
```

Pour en savoir plus, voir le **Guide de référence de la ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**.

Basculement de mode de contrôleur

Vous pouvez modifier la personnalité du contrôleur en passant du mode RAID au mode HBA. Le contrôleur fonctionne comme un contrôleur HBA, où les pilotes sont transmis par l'intermédiaire du système d'exploitation. Le changement de mode de contrôleur est une opération planifiée qui ne se produit pas en temps réel.

REMARQUE :

- Le mode HBA avancé prend en charge les disques physiques non RAID et tous les disques virtuels de niveau RAID.
- Il prend uniquement en charge la création des disques virtuels RAID0, RAID1 et RAID10.

Le mode avancé HBA offre les fonctionnalités suivantes :

- Créer des disques virtuels avec un niveau de RAID 0, 1 ou 10.
- Soumettre des disques non RAID à l'hôte.
- Configurer une stratégie de cache par défaut pour les disques virtuels comme l'écriture différée avec lecture anticipée.
- Configurer des disques virtuels et des disques non RAID comme périphériques de démarrage valides.
- Convertir automatiquement tous les disques non configurés à non RAID :
  - Au démarrage du système
  - À la réinitialisation du contrôleur
  - Lorsque des disques non configurés sont insérés à chaud

REMARQUE : La création ou l'importation de disques virtuels RAID 5, 6, 50 ou 60 ne sont pas prises en charge. En outre, en mode avancé HBA, les disques non RAID sont énumérés en premier dans l'ordre croissant, alors que les volumes RAID sont énumérés par ordre décroissant.

Avant de passer le mode du contrôleur de RAID à HBA, vérifiez ce qui suit :

- Le contrôleur RAID prend en charge le changement de mode de contrôleur. L'option de changement de mode de contrôleur n'est pas disponible sur les contrôleurs où la personnalité RAID nécessite une licence.
- Tous les disques virtuels doivent être effacés ou supprimés.
- Les disques de secours doivent être supprimés ou retirés.
- Les configurations étrangères doivent être supprimées ou effacées.
- Tous les disques physiques qui sont en état d'échec doivent être retirés ou la mémoire cache associée doit être effacée.
- Toute clé de sécurité locale associée à des SED doit être supprimée.
- Le contrôleur ne doit pas avoir un cache préservé.
- Vous disposez de privilèges de contrôle du serveur pour basculer le mode du contrôleur.

REMARQUE : Assurez-vous de sauvegarder la configuration étrangère, la clé de sécurité, les disques virtuels et les disques de secours avant de changer le mode car les données sont supprimées.

Exceptions lors du basculement du mode du contrôleur

La liste suivante présente les exceptions qui se produisent pendant la définition du mode du contrôleur via les interfaces iDRAC telles que l'interface Web et RACADM :

- Si le contrôleur PERC est en mode RAID, vous devez effacer tous les disques virtuels, disques de secours, configurations étrangères, clés de contrôleur ou cache préservé avant de le faire passer en mode HBA.
- Vous ne pouvez pas configurer d'autres opérations RAID pendant la définition du mode du contrôleur. Par exemple, si le contrôleur PERC est en mode RAID et que vous définissez la valeur en attente du PERC sur le mode HBA, et si vous tentez de définir l'attribut d'initialisation en arrière-plan (BGI), la valeur en attente n'est pas lancée.
- Lorsque vous basculez le contrôleur PERC du mode HBA au mode RAID, les disques restent en l'état non RAID et ne sont pas automatiquement définis sur l'état Prêt. De plus, l'attribut **RAIDEnhancedAutoImportForeignConfig** est automatiquement défini sur **Activé**.

La liste suivante présente les exceptions qui se produisent lors de la définition du mode de contrôleur à l'aide de la fonctionnalité de profil de configuration de serveur en utilisant l'interface RACADM :

- La fonction de profil de configuration de serveur vous permet d'effectuer la configuration de plusieurs opérations RAID en même temps que la configuration du mode du contrôleur. Par exemple, si le contrôleur PERC est en mode HBA, vous pouvez modifier le profil de configuration de serveur (SCP) d'exportation de façon à définir le mode du contrôleur sur RAID, à convertir les lecteurs à l'état Prêt et à créer un disque virtuel.
- Lors du changement de mode de RAID à HBA, l'attribut **RAIDaction pseudo** est défini sur Mise à jour (comportement par défaut). L'attribut s'exécute et crée un disque virtuel qui échoue. Le mode du contrôleur est modifié, cependant, la tâche se termine avec des erreurs. Pour éviter ce problème, vous devez indiquer, dans le fichier SCP et à l'aide d'un commentaire, que l'attribut RAIDaction doit être ignoré.
- Lorsque le contrôleur PERC est en mode HBA, si vous exécutez l'aperçu de l'importation sur le SCP d'exportation qui a été modifié pour définir le mode du contrôleur sur RAID et que vous tentez de créer un disque virtuel, la création du disque virtuel échoue. L'aperçu d'importation ne prend pas en charge la validation des opérations RAID d'empilage avec la modification du mode de contrôleur.

Permutation du mode du contrôleur à l'aide de l'interface Web iDRAC

Pour basculer le mode du contrôleur, effectuez les étapes suivantes :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Aperçu** > **Contrôleurs**.
2. Sur la page **Contrôleurs**, cliquez sur **Action** > **Modifier**.
   La colonne **Valeur actuelle** affiche le paramètre actuel du contrôleur.
3. Dans le menu déroulant, sélectionnez le mode de contrôleur vers lequel vous souhaitez basculer, puis cliquez sur **Appliquer au prochain redémarrage**.
   Redémarrez le système pour que la modification prenne effet.

Basculement du mode de contrôleur à l'aide de RACADM

Pour basculer le mode du contrôleur à l'aide de RACADM, exécutez les commandes suivantes :

- Pour afficher le mode actuel du contrôleur :

  ```
  $ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
  ```

  La sortie suivante s'affiche :

  ```
  RequestedControllerMode = NONE
  ```

- Pour définir le mode du contrôleur en tant que HBA :

  ```
  $ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
  ```

- Pour créer une tâche et appliquer les modifications :

  ```
  $ racadm jobqueue create <Controller Instance ID> -s TIME_NOW -r pwrcycle
  ```

Pour en savoir plus, voir le **Guide de référence de l'interface de ligne de commande RACADM iDRAC** disponible à l'adresse **dell.com/idracmanuals**.

Opérations de l'adaptateur HBA

Un système d'exploitation doit être installé sur les serveurs Dell PowerEdge ainsi qu'un pilote de périphérique approprié, afin que Dell HBA puisse fonctionner. Après l'auto-test de démarrage (POST), les ports HBA sont désactivés. Le pilote de périphérique HBA est responsable de la réinitialisation du HBA et de l'activation de ses ports qui sont connectés aux périphériques de stockage. Sans système d'exploitation, le pilote n'est pas chargé et il n'y a aucune garantie que l'iDRAC soit en mesure d'afficher les périphériques de stockage qui sont connectés aux adaptateurs Dell HBA.

Les contrôleurs non RAID sont les adaptateurs HBA ne disposant pas de certaines capacités RAID. Ils ne prennent pas en charge les disques virtuels.

Vous pouvez effectuer les opérations suivantes pour les contrôleurs non RAID :

- Affichez les propriétés applicables du contrôleur, des disques physiques et du boîtier pour le contrôleur non RAID. Affichez également les propriétés de l'EMM, du ventilateur, du bloc d'alimentation et du capteur de température associées au boîtier. Les propriétés s'affichent en fonction du type de contrôleur.
- Afficher les informations d'inventaire des logiciels et du matériel.
- Mettre à jour le firmware des boîtiers au dos du contrôleur HBA (intermédiaire)
- Surveiller l'interrogation ou la fréquence d'interrogation de l'état de déplacement SMART du disque physique lorsqu'un changement est détecté
- Surveiller l'état du retrait à chaud ou de l'enfichage à chaud des disques physiques
- Faire clignoter des voyants LED ou en arrêter le clignotement

REMARQUE :

- Même si le voyant LED n'est pas disponible pour le lecteur de bande, l'option faire clignoter/arrêter le clignotement peut aboutir.

REMARQUE :

- Activez l'option Collect System Inventory On Reboot (CSIOR) avant de faire l'inventaire ou de surveiller les contrôleurs non RAID.

REMARQUE : La détection de disques défaillants derrière les contrôleurs HBA SAS n'est pas prise en charge.

Surveillance de l'analyse de la prédiction d'échec sur des disques

Storage Management prend en charge la technologie SMART (Self Monitoring Analysis and Reporting Technology) sur les disques physiques compatibles SMART.

SMART effectue une analyse prédictive des pannes sur chaque disque et envoie des alertes si une panne de disque est prévue. Les contrôleurs vérifient les prévisions de panne des disques physiques et, en cas de panne détectée, transmettent ces informations à l'iDRAC. L'iDRAC enregistre immédiatement une alerte.

Opérations de contrôleur en mode non RAID ou HBA

Si le contrôleur est en mode non RAID (mode HBA), procédez comme suit :

- Les disques virtuels ou disques de secours ne sont pas disponibles.
- L'état de sécurité du contrôleur est désactivé.
- Tous les disques physiques sont en mode non RAID.

Vous pouvez effectuer les opérations suivantes si le contrôleur est en mode non RAID :

- Faire clignoter et arrêter le clignotement du disque physique.
- Configurez toutes les propriétés, notamment les suivantes :
  - Mode d'équilibrage de charge
  - Mode de vérification de la cohérence
  - Mode de lecture cohérente
  - Mode de recopie
  - Mode d'amorçage du contrôleur
  - Configuration étrangère d'importation automatique optimisée
  - Taux de recréation
  - Taux de vérification de la cohérence
  - Taux de reconstruction
  - Taux d'initialisation en arrière-plan (BGI)
  - Mode du boîtier ou du fond de panier
  - Zones non configurées de la lecture cohérente
- Afficher toutes les propriétés qui s'appliquent à un contrôleur RAID prévu pour les disques virtuels.
- Effacer la configuration étrangère

REMARQUE : Si une opération n'est pas prise en charge en mode non RAID, un message d'erreur s'affiche.

Vous ne pouvez pas surveiller les capteurs de température du boîtier, les ventilateurs et les blocs d'alimentation lorsque le contrôleur est en mode non RAID.

Exécution de tâches de configuration RAID sur plusieurs contrôleurs de stockage

Lors de l'exécution d'opérations sur plus de deux contrôleurs de stockage depuis n'importe quelle interface d'iDRAC, assurez-vous de :

- Exécuter les tâches sur chaque contrôleur individuellement. Attendez que chaque tâche se termine avant de démarrer la configuration et la création de la tâche sur le contrôleur suivant.
- Planifier plusieurs tâches à exécuter ultérieurement à l'aide des options de planification.

Gérer le cache conservé

La fonctionnalité Cache conservé géré est une option de contrôleur offrant à l'utilisateur la possibilité d'éliminer les données mises en cache du contrôleur. Dans la politique d'écriture différée, les données sont écrites dans le cache avant d'être écrites sur le disque physique. Si le disque virtuel est hors ligne ou est supprimé pour une raison quelconque, les données du cache sont éliminées.

Le contrôleur PERC conserve les données écrites sur le cache conservé ou encombré en cas de coupure d'alimentation ou de déconnexion du câble jusqu'à ce que vous récupériez le disque virtuel ou effaciez le cache.

L'état du contrôleur est affecté par le cache conservé. L'état du contrôleur s'affiche comme dégradé si le contrôleur a conservé sa mémoire cache. La suppression du cache conservé n'est possible que si toutes les conditions suivantes sont remplies :

- Le contrôleur ne présente aucune configuration étrangère.
- Le contrôleur ne présente pas de disques virtuels hors ligne ou manquants.
- Les câbles d'un disque virtuel ne sont pas déconnectés.

Gestion des SSD PCIe

Le périphérique SSD (Solid State Device) PCIe (Peripheral Component Interconnect Express) est un périphérique de stockage hautes performances conçu pour les solutions exigeant une faible latence et des opérations d'E/S par seconde (IOPS) élevées ainsi qu'une fiabilité et une facilité de maintenance du stockage d'entreprise. Le périphérique SSD PCIe est conçu à partir des technologies Flash NAND SLC (Single Level Cell) et (MLC), associées à une interface ultra-rapide conforme aux normes PCIe 2.0, PCIe 3.0 ou PCIe 4.0.

Utiliser les interfaces iDRAC, vous pouvez afficher et configurer les SSD PCIe NVMe.

Fonctionnalités clé du lecteur SSD PCIe :

- Fonctionnalité d'enfichage à chaud
- Périphérique hautes performance

Vous pouvez effectuer les opérations suivantes pour les SSD PCIe :

- Faire l'inventaire et surveiller à distance l'intégrité des SSD PCIe dans le serveur
- Se préparer à retirer le disque SSD PCIe
- Effacer les données en toute sécurité
- Faire clignoter ou arrêter le clignotement de la LED du périphérique (pour l'identifier)

Vous pouvez effectuer les opérations suivantes pour les SSD HHHL :

- Inventaire et surveillance en temps réel du disque SSD HHHL dans le serveur
- Rapports d'échecs de carte et de consignation dans l'iDRAC et OMSS
- Effacement en toute sécurité des données et retrait de la carte
- Rapports de fichiers journaux TTY

Vous pouvez effectuer les opérations suivantes pour les disques SSD :

- Rapport d'état du disque tel que En ligne, Échec, et Hors ligne

REMARQUE : La fonctionnalité d'enfichage à chaud, la préparation au retrait et le clignotement ou l'arrêt du clignotement de la LED du périphérique ne s'appliquent pas aux périphériques SSD PCIe HHHL.

REMARQUE : Lorsque les appareils NVMe sont contrôlés derrière le logiciel RAID, les opérations de préparation au retrait et d'effacement cryptographique ne sont pas prises en charge ; le clignotement et l'arrêt du clignotement sont cependant pris en charge.

Inventaire et surveillance de SSD PCIe

Les informations d'inventaire et de surveillance suivantes sont disponibles pour les SSD PCIe :

- Informations relatives au matériel :
  - Carte de l'extenseur SSD PCIe
  - Fond de panier SSD PCIe

    REMARQUE : Si le système est équipé d'un fond de panier PCIe dédié, deux FQDD sont affichés. Un FQDD est destiné aux lecteurs standard et l'autre aux disques SSD. Si le fond de panier est partagé (universel), un seul FQDD s'affiche. Dans le cas où les disques SSD sont directement connectés, le FQDD de contrôleur est affiché en tant que CPU.1, ce qui indique que le disque SSD est directement connecté à l'UC.
- L'inventaire des logiciels inclut uniquement la version du micrologiciel du SSD PCIe.

Inventaire et surveillance de SSD PCIe à l'aide de l'interface Web

Pour inventorier et surveiller les périphériques SSD PCIe, dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Disques physiques**. La fenêtre **Propriétés** s'affiche. Pour les cartes SSD PCIe, la colonne **Nom** affiche **SSD PCIe**. Développez la colonne pour afficher les propriétés.

Inventaire et surveillance de SSD PCIe à l'aide de RACADM

Pour afficher tous les disques SSD PCIe :

```
racadm storage get pdisks
```

Pour afficher les cartes d'extension PCIe :

```
racadm storage get controllers
```

Pour afficher les informations du fond de panier SSD PCIe :

```
racadm storage get enclosures
```

REMARQUE : Pour toutes les commandes mentionnées, les périphériques PERC sont également affichés.

Pour en savoir plus, voir le **Guide de référence de la ligne de commande RACADM d'iDRAC**, disponible sur **dell.com/idracmanuals**.

Préparation au retrait d'un SSD PCIe

REMARQUE : Cette opération n'est pas prise en charge lorsque :

- le disque SSD PCIe est configuré à l'aide du contrôleur S140 ;
- un périphérique NVMe se trouve derrière PERC 11.

Les périphériques SSD PCIe prennent en charge l'échange à chaud ordonné, ce qui vous permet d'ajouter ou de retirer un périphérique sans interrompre ou redémarrer le système dans lequel les périphériques se trouvent. Pour éviter la perte de données, vous devez utiliser l'opération de préparation au retrait avant d'effectuer le retrait physique d'un périphérique.

L'échange à chaud ordonné n'est pris en charge que lorsque les périphériques SSD PCIe sont installés dans un système Dell pris en charge exécutant un système d'exploitation pris en charge. Pour être sûr que vous disposez de la bonne configuration pour votre périphérique SSD PCIe, reportez-vous au Manuel du propriétaire correspondant au système.

L'opération de préparation au retrait n'est pas prise en charge pour les SSD PCIe sur les systèmes VMware vSphere (ESXi) et les périphériques SSD PCIe HHHL.

L'opération de préparation au retrait peut être effectuée en temps réel à l'aide d'iDRAC Service Module.

L'opération de préparation au retrait arrête toute activité en arrière-plan et toute activité d'E/S en cours, de sorte que le périphérique peut être retiré en toute sécurité. Elle fait clignoter les voyants d'état du périphérique. Vous pouvez retirer le périphérique du système en toute sécurité dans les conditions suivantes après avoir lancé l'opération de préparation au retrait :

- Le SSD PCIe clignote et suit la séquence de voyant LED signifiant qu'il peut être retiré en toute sécurité (clignote en orange).
- Le périphérique SSD PCIe n'est plus accessible au système.

Avant de préparer le SSD PCIe au retrait, assurez-vous que :

- L'iDRAC Service Module s'affiche.
- Le Lifecycle Controller est activé.
- Vous disposez des privilèges de contrôle et d'ouverture de session sur le serveur.

Préparation au retrait d'un SSD PCIe à l'aide de l'interface Web

Pour préparer le retrait du SSD PCIe :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Disques physiques**.
   La page **Sélectionner un disque physique** s'affiche.
2. Dans le menu déroulant **Contrôleur**, sélectionnez l'extenseur SSD PCIe pour afficher les SSD PCIe associés.
3. Dans les menus déroulants, sélectionnez **Préparer au retrait** d'un ou plusieurs SSD PCIe.
   Si vous avez sélectionné l'option **Prepare to Remove** , et que vous souhaitez afficher les autres options du menu déroulant, sélectionnez **Action**, puis cliquez sur le menu déroulant pour afficher les autres options.
   REMARQUE : Assurez-vous qu'iSM est installé et en cours d'exécution pour effectuer l'opération `preparetoremove`.

4. Dans le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez **Appliquer maintenant** pour appliquer les actions immédiatement.

   S'il existe des tâches à terminer, cette option est grisée.

   REMARQUE : Pour les appareils SSD PCIe, seule l'option **Appliquer maintenant** est disponible. Cette opération n'est pas prise en charge en mode échelonné.

5. Cliquez sur **Appliquer**.

   Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué s'affiche. De plus, l'ID du message et l'action de réponse recommandée s'affichent.

   Si la tâche est créée avec succès, un message indiquant que l'ID de tâche est créée sur le contrôleur sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page **File d'attente**.

   Si l'opération en attente n'est pas créée, un message d'erreur s'affiche. Si l'opération en attente aboutit mais que la création de la tâche échoue, un message d'erreur s'affiche.

Préparation au retrait d'un SSD PCIe à l'aide de RACADM

Pour préparer le retrait d'un SSD PCIe :

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

Pour créer la tâche cible après avoir exécuté la commande `preparetoremove` :

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

Pour rechercher l'ID de tâche renvoyée :

```
racadm jobqueue view -i <job ID>
```

Pour en savoir plus, voir le *Guide de l'interface de ligne de commande de référence RACADM*.

Effacement des données du périphérique SSD PCIe

REMARQUE : Cette opération n'est pas prise en charge lorsque le disque SSD PCIe est configuré à l'aide du contrôleur SWRAID.

La tâche Effacement du chiffrement efface définitivement toutes les données présentes sur le disque. Tout effacement cryptographique sur un disque SSD PCIe écrase tous les blocs et entraîne la perte définitive de toutes les données présentes sur ce périphérique. Pendant l'effacement cryptographique, l'hôte ne peut pas accéder au disque SSD PCIe. Les modifications sont appliquées après le redémarrage du système.

Si le système redémarre ou subit une perte de puissance au cours d'un effacement cryptographique, l'opération est annulée. Vous devez redémarrer le système et recommencer le processus.

Avant d'effacer les données du périphérique SSD PCIe, assurez-vous que :

- Le Lifecycle Controller est activé.
- Vous disposez des privilèges de contrôle et d'ouverture de session sur le serveur.

REMARQUE :

- L'effacement des disques SSD PCIe ne peut être effectuée qu'en tant qu'opération différée.
- Une fois le disque effacé, il s'affiche dans le système d'exploitation comme étant en ligne, mais il n'est pas initialisé. Vous devez initialiser et formater le disque avant de l'utiliser à nouveau.
- Une fois un SSD PCIe enfiché à chaud, il peut mettre quelques secondes à s'afficher dans l'interface web.

Effacement des données d'un périphérique SSD PCIe à l'aide de l'interface Web

Pour effacer les données du périphérique SSD PCIe :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Disques physiques**.
   La page **Disques physiques** s'affiche.

2. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur pour afficher les SSD PCIe associés.
3. Dans les menus déroulants, sélectionnez **Effacement cryptographique** pour une ou plusieurs cartes SSD PCIe.

   Si vous avez sélectionné **Effacement cryptographique** et que vous souhaitez afficher les autres options du menu déroulant, sélectionnez **Action**, puis cliquez sur le menu déroulant pour afficher les autres options.
4. Dans le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez l'une des options suivantes :
   - **Au prochain redémarrage** : cette option permet d'appliquer les actions lors du prochain redémarrage système.
   - **À l'heure programmée** : sélectionnez cette option pour appliquer les actions à un jour et à une heure planifiés :
     - **Heure de début** et **Heure de fin** : cliquez sur les icônes de calendrier et sélectionnez les dates. Dans les menus déroulants, sélectionnez l'heure. L'action est appliquée entre l'heure de début et l'heure de fin.
     - Dans le menu déroulant, sélectionnez le type de redémarrage :
       - Pas de redémarrage (Redémarrage manuel du système)
       - Arrêt normal
       - Arrêt forcé
       - Exécuter un cycle d'alimentation du système (démarrage à froid)
5. Cliquez sur **Appliquer**.

   Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué s'affiche. De plus, l'ID du message et l'action de réponse recommandée s'affichent.

   Si la tâche est créée avec succès, un message indiquant que l'ID de tâche est créée sur le contrôleur sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page File d'attente.

   Si l'opération en attente n'est pas créée, un message d'erreur s'affiche. Si l'opération en attente aboutit mais que la création de la tâche échoue, un message d'erreur s'affiche.

Effacement des données d'un périphérique SSD PCIe à l'aide de RACADM

Pour effacer en toute sécurité un SSD PCIe :

```
racadm storage secureerase:<PCIeSSD FQDD>
```

Pour créer la tâche cible après avoir exécuté la commande `secureerase` :

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

Pour rechercher l'ID de tâche renvoyée :

```
racadm jobqueue view -i <job ID>
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM d'iDRAC*.

Gestion des boîtiers ou des fonds de panier

Vous pouvez effectuer les opérations suivantes pour les boîtiers ou fonds de panier :

- Afficher les propriétés
- Configurer le mode universel ou mode divisé
- Afficher les informations sur le logement (universel ou partagé)
- Définir le mode SGPIO
- Configurer le numéro d'inventaire
- Nom de l'actif

Configuration du mode du fond de panier

Les serveurs PowerEdge prennent en charge une nouvelle topologie de stockage interne, dans laquelle deux contrôleurs de stockage (PERC) peuvent être connectés à des disques internes à l'aide d'un seul module d'extension. Cette configuration est utilisée pour le mode hautes performances sans basculement ou la fonctionnalité de haute disponibilité (HA). L'extenseur répartit la baie de disques internes entre les deux contrôleurs de stockage. Dans ce mode, la création de disques virtuels affiche uniquement les disques connectés à un

contrôleur particulier. Cette fonctionnalité ne nécessite aucune licence. Cette fonctionnalité est prise en charge uniquement sur quelques systèmes.

Le fond de panier prend en charge les modes suivants :

- Mode unifié : il s'agit du mode par défaut. Le contrôleur PERC principal a accès à tous les disques connectés au fond de panier, même si un deuxième contrôleur PERC est installé.
- Mode fractionné : un contrôleur a accès aux 12 premiers disques et le second contrôleur a accès aux 12 derniers disques. Les disques connectés au premier contrôleur sont numérotés de 0 à 11, tandis que les disques connectés au second contrôleur sont numérotés de 12 à 23.
- Mode fractionné 4:20 : un contrôleur a accès aux quatre premiers disques et le second contrôleur a accès aux 20 derniers disques. Les disques connectés au premier contrôleur sont numérotés de 0 à 3, tandis que les disques connectés au second contrôleur sont numérotés de 4 à 23.
- Mode fractionné 8:16 : un contrôleur a accès aux huit premiers disques et le second contrôleur a accès aux 16 derniers disques. Les disques connectés au premier contrôleur sont numérotés de 0 à 7, tandis que les disques connectés au second contrôleur sont numérotés de 8 à 23.
- Mode fractionné 16:8 : un contrôleur a accès aux 16 premiers disques et le second contrôleur a accès aux huit derniers disques. Les disques connectés au premier contrôleur sont numérotés de 0 à 15, tandis que les disques connectés au second contrôleur sont numérotés de 16 à 23.
- Mode fractionné 20:4 : un contrôleur a accès aux 20 premiers disques et le second contrôleur a accès aux quatre derniers disques. Les disques connectés au premier contrôleur sont numérotés de 0 à 19, tandis que les disques connectés au second contrôleur sont numérotés de 20 à 23.
- Informations non disponibles : les informations de contrôleur ne sont pas disponibles.

L'iDRAC permet de définir le mode fractionné si l'extenseur est en mesure de prendre en charge la configuration. Assurez-vous d'activer ce mode avant d'installer le deuxième contrôleur. L'iDRAC vérifie la capacité du module d'extension avant d'autoriser la configuration de ce mode et ne vérifie pas si le deuxième contrôleur PERC est présent.

REMARQUE : Des erreurs de câble (ou autres) peuvent se produire si vous placez le fond de panier en mode fractionné en y connectant un seul contrôleur PERC ou si vous le placez en mode unifié en y connectant deux contrôleurs PERC.

REMARQUE : Lorsque deux fonds de panier ou plus sont connectés à un seul contrôleur PERC, le contrôleur les combine et les affiche en tant que boîtier unique. Par conséquent, vous ne devriez voir qu'un seul fond de panier dans l'inventaire matériel ou sur la page Stockage. L'inventaire du firmware indique le nombre réel de fonds de panier présents dans le système.

Pour modifier le paramètre, vous devez disposer des privilèges de contrôle du serveur.

Si d'autres opérations RAID sont en attente ou si une tâche RAID est planifiée, vous ne pouvez pas modifier le mode fond de panier. De même, si ce paramètre est en attente, vous ne pouvez pas planifier d'autres tâches RAID.

REMARQUE :

- Des messages d'avertissement s'affichent lorsque le paramètre est en cours de modification car il y a un risque de perte de données.
- Les opérations de suppression de LC ou de réinitialisation d'iDRAC ne modifient pas la configuration de l'extenseur de ce mode.
- Cette opération est prise en charge uniquement en temps réel et n'est pas différée.
- Vous pouvez modifier la configuration du fond de panier plusieurs fois.
- Si le fond de panier est configuré avec l'attribut **Logements physiques 0**, l'iDRAC HII n'affiche pas les détails du fond de panier.
- L'opération de fractionnement du fond de panier peut entraîner une perte de données ou une configuration étrangère si l'association de lecteurs change d'un contrôleur à un autre.
- Au cours de l'opération de fractionnement du fond de panier, la configuration RAID peut être affectée en fonction de l'association de lecteurs.

Toute modification de ce paramètre ne prend effet qu'après une réinitialisation d'alimentation du système. Si vous passez du mode unifié au mode divisé, un message d'erreur s'affiche au prochain démarrage car le second contrôleur ne voit aucun disque. En outre, le premier contrôleur voit une configuration étrangère. Si vous ignorez cette erreur, les disques virtuels existants sont perdus.

Configuration du boîtier à l'aide de RACADM

Pour configurer le boîtier ou le fond de panier, utilisez la commande `set` avec les objets dans **BackplaneMode**.

Par exemple, pour définir l'attribut BackplaneMode sur le mode partagé :

1. Exécutez la commande suivante pour afficher le mode fond de panier actuel :

   ```
   racadm get storage.enclosure.1.backplanecurrentmode
   ```

   Le résultat est :

   ```
   BackplaneCurrentMode=UnifiedMode
   ```

2. Exécutez la commande suivante pour afficher le mode requis :

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   Le résultat est :

   ```
   BackplaneRequestedMode=None
   ```

3. Exécutez la commande suivante pour définir le mode du fond de panier sur le mode partagé :

   ```
   racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
   ```

   Le message s'affiche, indiquant que l'exécution de la commande a réussi.

4. Exécutez la commande suivante pour vérifier si l'attribut **backplanerequestedmode** est défini sur le mode partagé :

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   Le résultat est :

   ```
   BackplaneRequestedMode=None (Pending=SplitMode)
   ```

5. Exécutez la commande `storage get controllers` et prenez note de l'ID de l'instance du contrôleur
6. Exécutez la commande suivante pour créer une tâche :

   ```
   racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
   ```

   Un ID de tâche est renvoyé.

7. Exécutez la commande suivante pour interroger l'état de la tâche :

   ```
   racadm jobqueue view -i JID_xxxxxxxx
   ```

   où `JID_xxxxxxxx` représente l'ID de la tâche de l'étape 6.

   L'état est affiché comme En attente.

   Continuez à interroger l'ID de tâche jusqu'à ce que l'état Terminé s'affiche (ce processus peut prendre jusqu'à trois minutes).

8. Exécutez la commande suivante pour afficher la valeur de l'attribut `backplanerequestedmode` :

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   Le résultat est :

   ```
   BackplaneRequestedMode=SplitMode
   ```

9. Exécutez la commande suivante pour redémarrer le serveur à froid :

   ```
   racadm serveraction powercycle
   ```

10. Lorsque le système a terminé les opérations POST et CSIOR, saisissez la commande suivante pour vérifier l'attribut `backplanerequestedmode` :

    ```
    racadm get storage.enclosure.1.backplanerequestedmode
    ```

Le résultat est :

```
BackplaneRequestedMode=None
```

11. Exécutez la commande suivante pour vérifier pourquoi le mode du fond de panier est défini sur le mode partagé :

```
racadm get storage.enclosure.1.backplanecurrentmode
```

Le résultat est :

```
BackplaneCurrentMode=SplitMode
```

12. Exécutez la commande suivante et vérifiez que seuls les disques 0 à 11 sont affichés :

```
racadm storage get pdisks
```

Pour plus d'informations sur les commandes RACADM, voir le **Guide de référence de l'interface de ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**.

Configuration du mode du fond de panier à l'aide de l'interface Web

Pour configurer le mode du fond de panier à l'aide de l'interface Web iDRAC :

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Boîtiers**.
2. Dans l'option **Boîtier**, sélectionnez le boîtier à configurer.
3. À partir du menu déroulant **Action**, sélectionnez **Modifier le mode de boîtiers**.
   La page **Modifier le mode de boîtiers** s'affiche.
4. Dans la colonne **Valeur actuelle**, sélectionnez le mode de boîtiers requis pour le fond de panier ou le boîtier. Les options sont les suivantes :
   - Mode unifié
   - Mode fractionné
   - Mode fractionné 4:20
   - Mode fractionné 8:16
   - Mode fractionné 16:8
   - Mode fractionné 20:4
5. Cliquez sur **Ajouter aux opérations en attente**.
   Un ID de tâche est créé.
6. Cliquez sur **Appliquer maintenant**.
7. Accédez à la page **File d'attente des tâches** et vérifiez que la tâche affiche l'état Terminé.
8. Effectuez un cycle d'alimentation sur le système pour que la configuration soit appliquée.

   REMARQUE : Pour éviter les problèmes d'inventaire, en cas de modification de la connexion des câbles du fond de panier, vous devez redémarrer l'iDRAC et effectuer un cycle d'alimentation pour l'hôte.

Définition du mode SGPIO

Le contrôleur de stockage peut se connecter au fond de panier en mode I2C (paramètre par défaut pour les fonds de panier Dell) ou en mode entrée/sortie série à usage général (SGPIO). Cette connexion est obligatoire pour faire clignoter les LED sur les disques. Les contrôleurs PERC Dell et le fond de panier prennent en charge ces deux modes. Pour prendre en charge certains adaptateurs de canal, le mode de fond de panier doit être modifié en mode SGPIO.

Le mode SGPIO est uniquement pris en charge pour les fonds de panier passifs. Il n'est pas pris en charge pour les fonds de panier basés sur un module d'extension ou les fonds de panier passifs en mode descendant. Le firmware du fond de panier fournit des informations sur la fonctionnalité, l'état actuel et l'état demandé.

Après l'opération de suppression de LC ou la réinitialisation d'iDRAC, le mode SGPIO est réinitialisé à l'état désactivé. Il compare le paramètre d'iDRAC avec le paramètre du fond de panier. Si le fond de panier est défini sur le mode SGPIO, iDRAC change son paramètre pour qu'il corresponde au paramètre du fond de panier.

Le cycle d'alimentation du serveur est nécessaire pour qu'une modification de paramètre prenne effet.

Vous devez disposer du privilège de contrôle du serveur pour modifier ce paramètre.

REMARQUE : Vous ne pouvez pas modifier le mode SGPIO à l'aide de l'interface Web d'iDRAC.

Définition du mode SGPIO à l'aide de RACADM

Pour configurer le mode SGPIO, utilisez la commande `set` avec les objets du groupe `SGPIOMode`.

Si cette option est désactivée, il s'agit du mode I2C. Si cette option est activée, il s'agit du mode SGPIO.

Pour en savoir plus, voir le **Guide de référence de l'interface de ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**.

Définition du nom d'inventaire d'un boîtier

Définir le nom d'inventaire d'un boîtier permet à l'utilisateur de configurer le nom d'inventaire d'un boîtier de stockage.

L'utilisateur peut modifier la propriété Nom d'inventaire du boîtier pour identifier facilement les boîtiers. Ces champs sont vérifiés pour détecter les valeurs non valides, et une erreur s'affiche en cas de saisie d'une valeur incorrecte. Ces champs font partie du firmware du boîtier ; les données initialement affichées sont les valeurs enregistrées dans le firmware.

REMARQUE : Le nom d'inventaire peut comporter 32 caractères maximum, dont le caractère nul.

REMARQUE : Ces opérations ne sont pas prises en charge sur les boîtiers internes.

Définition du numéro d'inventaire d'un boîtier

Définir le numéro d'inventaire d'un boîtier vous permet de configurer le numéro d'inventaire d'un boîtier de stockage.

L'utilisateur peut modifier la propriété Numéro d'inventaire du boîtier pour identifier les boîtiers. Ces champs sont vérifiés pour détecter les valeurs non valides, et une erreur s'affiche en cas de saisie d'une valeur incorrecte. Ces champs font partie du firmware du boîtier ; les données initialement affichées sont les valeurs enregistrées dans le firmware.

REMARQUE : Le numéro d'inventaire peut comporter 10 caractères maximum, dont le caractère nul.

REMARQUE : Ces opérations ne sont pas prises en charge sur les boîtiers internes.

Choix du mode de fonctionnement pour l'application des paramètres

Lors de la création et la gestion des disques virtuels, la configuration des disques physiques, contrôleurs et boîtiers ou la réinitialisation des contrôleurs, avant d'appliquer les paramètres, vous devez sélectionner le mode de fonctionnement. Autrement dit, spécifiez le moment où vous souhaitez appliquer les paramètres :

- Immédiatement
- Lors du prochain redémarrage du système
- À une heure planifiée
- Dans le cadre d'une opération en attente devant être appliquée sous la forme d'un lot dans le cadre d'une tâche unique.

Choix du mode de fonctionnement à l'aide de l'interface Web

Pour sélectionner le mode de fonctionnement à appliquer aux paramètres :

1. Vous pouvez sélectionner le mode de fonctionnement lorsque vous vous trouvez sur l'une des pages suivantes :
   - **Stockage** > **Disques physiques**
   - **Stockage** > **Disques virtuels**
   - **Stockage** > **Contrôleurs**
   - **Stockage** > **Boîtiers**
2. Sélectionnez l'une des options suivantes du menu déroulant **Appliquer le mode de fonctionnement** :

- **Au prochain redémarrage** : sélectionnez cette option pour appliquer les paramètres lors du prochain redémarrage système.
- **À l'heure programmée** : sélectionnez cette option pour appliquer les paramètres à un jour et à une heure planifiés :
  - **Heure de début** et **Heure de fin** : cliquez sur les icônes de calendrier et sélectionnez les dates. Dans les menus déroulants, sélectionnez l'heure. Les paramètres sont appliqués entre l'heure de début et l'heure de fin.
  - Dans le menu déroulant, sélectionnez le type de redémarrage :
    - Pas de redémarrage (Redémarrage manuel du système)
    - Arrêt normal
    - Arrêt forcé
    - Exécuter un cycle d'alimentation du système (démarrage à froid)
- **Ajouter aux opérations en attente** : sélectionnez cette option pour créer une opération en attente pour appliquer les paramètres. Vous pouvez afficher toutes les opérations en attente d'un contrôleur dans la page **Stockage** > **Présentation** > **Opérations en attente**.

REMARQUE :
- L'option **Ajouter aux opérations en attente** n'est pas applicable à la page **Opérations en attente** pour les SSD PCIe sur la page **Disques physiques** > **Configuration**.
- Seule l'option **Appliquer maintenant** est disponible sur la page **Configuration du boîtier**.

3. Cliquez sur **Appliquer**.
   Les paramètres sont appliqués en fonction du mode de fonctionnement sélectionné.

Choix du mode de fonctionnement à l'aide de RACADM

Pour sélectionner le mode de fonctionnement, utilisez la commande `jobqueue`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Affichage et application des opérations en attente

Vous pouvez afficher et valider toutes les opérations en attente du contrôleur de stockage. Tous les paramètres sont appliqués en une seule fois, au cours du prochain redémarrage ou à une heure planifiée, selon les options sélectionnées. Vous pouvez supprimer toutes les opérations en attente d'un contrôleur. Vous ne pouvez pas supprimer les opérations en attente individuelles.

Les opérations en attente sont créées sur les composants sélectionnés (contrôleurs, boîtiers, disques physiques et disques virtuels).

Les tâches de configuration sont créées uniquement sur le contrôleur. Dans le cas des disques SSD PCIe, la tâche est créée sur un disque SSD PCIe et non sur la carte d'extension PCIe.

Affichage, application ou suppression des opérations en attente à l'aide de l'interface Web

1. Dans l'interface Web de l'iDRAC, accédez à **Stockage** > **Présentation** > **Opérations en attente**.
   La page **Opérations en attente** s'affiche.
2. Dans le menu déroulant **Composant**, sélectionnez le contrôleur dont vous souhaitez afficher, valider ou supprimer les opérations en attente.
   La liste des opérations en attente s'affiche pour le contrôleur sélectionné.

   REMARQUE :
   - Des opérations en attente sont créées pour l'importation d'une configuration étrangère, la suppression d'une configuration étrangère, les opérations de clé de sécurité et le chiffrement de disques virtuels. Toutefois, elles ne s'affichent pas dans la page **Opérations en attente** et dans le message contextuel Opérations en attente.
   - Les tâches du SSD PCIe ne peuvent pas être créées à partir de la page **Opérations en attente**
3. Pour supprimer les opérations en attente pour le contrôleur sélectionné, cliquez sur **Supprimer toutes les opérations en attente**.
4. Dans le menu déroulant, sélectionnez l'une des options suivantes et cliquez sur **Appliquer** pour valider les opérations en attente :
   - **Au prochain redémarrage** : sélectionnez cette option pour valider toutes les opérations lors du prochain redémarrage système.
   - **À un moment planifié** : sélectionnez cette option pour valider les opérations à un jour et à une heure planifiés.
     - **Heure de début** et **Heure de fin** : cliquez sur les icônes de calendrier et sélectionnez les dates. Dans les menus déroulants, sélectionnez l'heure. L'action est appliquée entre l'heure de début et l'heure de fin.

- Dans le menu déroulant, sélectionnez le type de redémarrage :
  - Pas de redémarrage (Redémarrage manuel du système)
  - Arrêt normal
  - Arrêt forcé
  - Exécuter un cycle d'alimentation du système (démarrage à froid)

5. Si la tâche de validation n'est pas créée, un message indiquant que la création de tâche a échoué apparaît. De plus, l'ID du message et l'action recommandée s'affichent.
6. Si la tâche de validation est créée avec succès, un message indiquant que l'ID de tâche est créée sur le contrôleur sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page **File d'attente**.

   Si les opérations d'effacement de configuration étrangère, d'importation de configuration étrangère, de clé de sécurité ou de chiffrement de disque virtuel sont en attente, et s'il s'agit des seules opérations en attente, vous ne pouvez pas créer de tâche à partir de la page **Opérations en attente**. Vous devez exécuter une autre opération de configuration du stockage ou utiliser RACADM pour créer la tâche de configuration nécessaire sur le contrôleur requis.

   Vous ne pouvez pas afficher ou effacer les opérations en attente pour les disques SSD PCIe sur la page **Opérations en attente**. Utilisez la commande RACADM pour effacer les opérations en attente pour les disques SSD PCIe.

Affichage et application des opérations en attente à l'aide de RACADM

Pour appliquer des opérations en attente, utilisez la commande **jobqueue**.

Pour plus d'informations, voir le **Guide de référence de la ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**

Périphériques de stockage : scénarios d'opérations d'application

Cas 1 : une application d'opération a été sélectionnée (Appliquer maintenant, Au prochain redémarrage ou À l'heure planifiée) et il n'existe aucune opération en attente

Si vous avez sélectionné **Appliquer maintenant**, **Au prochain redémarrage**, ou **À l'heure planifiée** et que vous cliquez sur **Appliquer**, l'opération en attente est d'abord créée pour l'opération de configuration du stockage sélectionnée.

- Si l'opération en attente réussit et qu'aucune opération antérieure n'est en attente, la tâche est créée. Si la tâche est créée avec succès, un message indiquant que l'ID de tâche est créée sur le périphérique sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page **File d'attente**. Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué s'affiche. De plus, l'ID du message et l'action recommandée s'affichent.
- Si l'opération en attente de création échoue et qu'aucune opération antérieure n'est en attente, un message d'erreur contenant l'ID et l'action de réponse recommandée s'affiche.

Cas 1 : une opération d'application a été sélectionnée (Appliquer maintenant, Au prochain redémarrage ou À l'heure planifiée) et il existe des opérations en attente

Si vous avez sélectionné **Appliquer maintenant**, **Au prochain redémarrage** ou **À l'heure planifiée** et que vous cliquez sur **Appliquer**, l'opération en attente est d'abord créée pour l'opération de configuration du stockage sélectionnée.

- Si l'opération en attente est correctement créée et qu'il existe des opérations en attente, un message s'affiche.
  - Cliquez sur le lien **Afficher les opérations en attente** pour afficher les opérations en attente du périphérique.
  - Cliquez sur **Créer une tâche** pour créer une tâche pour le périphérique sélectionné. Si la tâche est créée avec succès, un message indiquant que l'ID de tâche est créée sur le périphérique sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page **File d'attente**. Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué s'affiche. De plus, l'ID du message et l'action de réponse recommandée s'affichent.
  - Cliquez sur **Annuler** pour ne pas créer la tâche et rester sur la page afin d'effectuer davantage d'opérations de configuration du stockage.
- Si l'opération en attente n'est pas correctement créée et qu'il existe des opérations en attente, un message d'erreur s'affiche.
  - Cliquez sur **Opérations en attente** pour afficher les opérations en attente du périphérique.
  - Cliquez sur **Créer une tâche pour les opérations réussies** pour créer la tâche pour les opérations en attente existantes. Si la tâche est créée avec succès, un message indiquant que l'ID de tâche est créée sur le périphérique sélectionné s'affiche. Cliquez sur **File d'attente** pour visualiser l'avancement de la tâche dans la page **File d'attente**. Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué s'affiche. De plus, l'ID du message et l'action recommandée s'affichent.

- Cliquez sur **Annuler** pour ne pas créer la tâche et rester sur la page afin d'effectuer davantage d'opérations de configuration du stockage.

Cas 3 : l'option Ajouter aux opérations en attente a été sélectionnée et il n'existe aucune opération en attente

Si vous avez sélectionné **Ajouter aux opérations en attente** et que vous avez cliqué sur **Appliquer**, l'opération en attente est d'abord créée pour l'opération de configuration du stockage sélectionnée.

- Si l'opération en attente est créée correctement et qu'il n'existe aucune opération en attente, un message d'erreur s'affiche.
  - Cliquez sur **OK** pour rester sur la page afin d'effectuer davantage d'opérations de configuration du stockage.
  - Cliquez sur **Opérations en attente** pour afficher les opérations en attente du périphérique. Tant que la tâche n'est pas créée sur le contrôleur sélectionné, ces opérations en attente ne sont pas appliquées.
- Si l'opération en attente n'est pas créée correctement et qu'il n'existe aucune opération en attente, un message d'erreur s'affiche.

Cas 4 : l'option Ajouter aux opérations en attente a été sélectionnée et il existe déjà des opérations en attente

Si vous avez sélectionné **Ajouter aux opérations en attente** et que vous avez cliqué sur **Appliquer**, l'opération en attente est d'abord créée pour l'opération de configuration du stockage sélectionnée.

- Si l'opération en attente est créée correctement et qu'il existe des opérations en attente, un message informatif s'affiche :
  - Cliquez sur **OK** pour rester sur la page afin d'effectuer davantage d'opérations de configuration du stockage.
  - Cliquez sur **Opérations en attente** pour afficher les opérations en attente du périphérique.
- Si l'opération en attente n'est pas correctement créée et qu'il existe des opérations en attente, un message d'erreur s'affiche.
  - Cliquez sur **OK** pour rester sur la page afin d'effectuer davantage d'opérations de configuration du stockage.
  - Cliquez sur **Opérations en attente** pour afficher les opérations en attente du périphérique.

REMARQUE :

- À tout moment, si vous ne voyez pas l'option de création d'une tâche dans les pages de configuration du stockage, accédez à la page **Présentation du stockage** > **Opérations en attente** pour afficher les opérations en attente existantes et pour créer la tâche sur le contrôleur requis.
- Seuls les cas 1 et 2 s'appliquent aux disques SSD PCIe. Vous ne pouvez pas afficher les opérations en attente pour les disques SSD PCIe ; par conséquent, l'option **Ajouter aux opérations en attente** n'est pas disponible. Utilisez la commande racadm pour effacer les opérations en attente pour les disques SSD PCIe.

Clignotement ou annulation du clignotement des LED des composants

Vous pouvez localiser un disque physique, un lecteur de disque virtuel et des SSD PCIe dans un boîtier en faisant clignoter l'un des voyants LED du disque.

Vous devez disposer de droits de connexion, de contrôle et de configuration du système pour activer ou désactiver le clignotement d'un voyant.

Le contrôleur doit pouvoir être configurable en temps réel. La prise en charge en temps réel de cette fonctionnalité est disponible uniquement dans le firmware PERC 9.1 et versions ultérieures.

REMARQUE : Le clignotement ou l'annulation du clignotement n'est pas pris en charge sur les serveurs sans fond de panier.

Faire clignoter ou arrêter le clignotement des LED des composants à l'aide de l'interface Web

Pour activer ou désactiver le clignotement d'un LED de composant :

1. Dans l'interface Web d'iDRAC, accédez à l'une des pages suivantes selon vos besoins :
   - **Stockage** > **Présentation** > **Disques physiques** > **État** : affiche la page Disques physiques identifiés, où vous pouvez activer ou désactiver le clignotement des disques physiques et des cartes SSD PCIe.
   - **Stockage** > **Présentation** > **Disques virtuels** > **État** : affiche la page Disques physiques identifiés, où vous pouvez activer ou désactiver le clignotement des disques virtuels.
2. Si vous sélectionnez le disque physique :

- Sélectionner ou désélectionner tous les voyants LED des composants : sélectionnez l'option **Sélectionner/Désélectionner tout**, puis cliquez sur **Clignotement** pour démarrer le clignotement des voyants LED des composants. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des voyants LED des composants.
- Sélectionnez ou désélectionnez des voyants LED de composants individuels : sélectionnez un ou plusieurs voyants LED de composants et cliquez sur **Clignotement** pour démarrer le clignotement de la/des voyants LED du/des composant(s) sélectionné(s). De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des voyants LED des composants.

3. Si vous sélectionnez le disque virtuel :
   - Sélectionnez ou désélectionnez tous les lecteurs de disque physique ou les cartes SSD PCIe : sélectionnez l'option **Sélectionner/Désélectionner tout**, puis cliquez sur **Clignotement** pour démarrer le clignotement sur tous les lecteurs de disque physique et les cartes SSD PCIe. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des LED.
   - Sélectionnez ou désélectionnez les disques physiques individuels ou de périphériques SSD PCIe : sélectionnez un ou plusieurs lecteurs de disque physique et cliquez sur **Clignotement** pour démarrer le clignotement des DEL des lecteurs de disque physique ou des périphériques SSD PCIe. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des LED.
4. Si vous êtes sur la page **Identifier les disques physiques** :
   - Sélectionnez ou désélectionnez tous les disques virtuels : sélectionnez l'option **Sélectionner/Désélectionner tout**, puis cliquez sur **Clignotement** pour faire clignoter les LED de l'ensemble des disques virtuels. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des LED.
   - Sélectionnez ou désélectionnez des disques virtuels : sélectionnez un ou plusieurs disques virtuels et cliquez sur **Clignotement** pour démarrer le clignotement des LED des disques virtuels. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des LED.

   Si l'opération d'activation ou de désactivation du clignotement échoue, un message d'erreur s'affiche.

Activation ou désactivation du clignotement des LED des composants à l'aide de RACADM

Pour activer ou désactiver le clignotement des LED des composants, utilisez les commandes suivantes :

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

Pour en savoir plus, voir le **Guide de référence de la ligne de commande RACADM iDRAC**, disponible sur **dell.com/idracmanuals**.

Redémarrage à chaud

Une fois le redémarrage à chaud effectué, vous observez les comportements suivants :

- Les contrôleurs PERC de l'interface utilisateur de l'iDRAC sont immédiatement grisés après le redémarrage à chaud. Ils sont disponibles une fois le nouvel inventaire terminé après un redémarrage à chaud. Cela s'applique uniquement aux contrôleurs PERC et non à NVME/HBA/BOSS.
- Dans SupportAssist, les fichiers de stockage sont vides lorsque les contrôleurs PERC sont grisés dans l'interface utilisateur graphique.
- La journalisation LC pour les événements passés et critiques est exécutée pour PERC pendant l'opération `perc reinventory`. Tous les autres LCL des composants PERC sont supprimés. LCL redémarre une fois le nouvel inventaire PERC terminé.
- Vous ne pouvez pas démarrer une tâche en temps réel tant que le nouvel inventaire PERC n'est pas terminé.
- Les données de télémétrie ne sont pas collectées avant la fin du nouvel inventaire PERC.
- Une fois l'inventaire PERC terminé, le comportement est normal.

REMARQUE : Après avoir effectué un démarrage à chaud du serveur, l'iDRAC peut signaler un message `Disk Inserted` dans les journaux LC pour les disques qui se trouvent derrière l'adaptateur HBA. Ignorez cette entrée de journal.

20

BIOS Settings (Paramètres SATA)

Vous pouvez afficher plusieurs attributs qui sont en cours d'utilisation pour un serveur spécifique sous les paramètres du BIOS. Vous pouvez modifier les différents paramètres de chaque attribut à partir de ce paramètre de la configuration du BIOS. Lorsque vous sélectionnez un attribut, il affiche différents paramètres liés à cet attribut spécifique. Vous pouvez modifier plusieurs paramètres d'un attribut et appliquer des modifications avant de modifier un autre attribut. Lorsqu'un utilisateur développe un groupe de configurations, les attributs sont affichés dans l'ordre alphabétique.

REMARQUE : Le contenu de l'aide au niveau de l'attribut est généré dynamiquement.

Appliquer

Le bouton **Appliquer** reste grisé jusqu'à ce qu'un des attributs soit modifié. Après avoir modifié un attribut, cliquez sur **appliquer**. L'attribut est modifié avec les modifications requises. Si la demande ne parvient pas à définir l'attribut BIOS, un message d'erreur s'affiche. Pour plus d'informations, reportez-vous au *Guide de référence : Messages d'erreur et d'événement des serveurs PowerEdge Dell Technologies 17G, 16G, 15G, 14G et 13G* disponible sur le site de support Dell.

Annuler les modifications

Le bouton **Annuler les modifications** est grisé jusqu'à ce qu'un des attributs soit modifié. Si vous cliquez sur le bouton **Annuler les modifications**, toutes les modifications récentes sont annulées et les valeurs précédentes ou initiales sont rétablies.

Appliquer et redémarrer

Lorsqu'un utilisateur modifie la valeur d'un attribut ou une séquence de démarrage, il se voit proposer deux choix pour appliquer la configuration : **Appliquer et redémarrer** ou **Appliquer au redémarrage suivant**. Quelle que soit l'option choisie, l'utilisateur est redirigé vers la page de file d'attente des tâches afin de surveiller la progression de cette tâche spécifique.

L'utilisateur peut visualiser des informations d'audit relatives à la configuration du BIOS dans les journaux LC.

Si vous cliquez sur **Appliquer et redémarrer**, le serveur redémarre immédiatement pour configurer toutes les modifications nécessaires. Si la demande ne parvient pas à définir les attributs du BIOS, un message d'erreur s'affiche.

Appliquer au redémarrage suivant

Lorsqu'un utilisateur modifie la valeur d'un attribut ou une séquence de démarrage, il se voit proposer deux choix pour appliquer la configuration : **Appliquer et redémarrer** ou **Appliquer au redémarrage suivant**. Quelle que soit l'option choisie, l'utilisateur est redirigé vers la page de file d'attente des tâches afin de surveiller la progression de cette tâche spécifique.

L'utilisateur peut visualiser des informations d'audit relatives à la configuration du BIOS dans les journaux LC.

Si vous cliquez sur **Appliquer au redémarrage suivant**, toutes les modifications requises sont configurées lors du prochain redémarrage du serveur. Vous ne constaterez aucune modification immédiate basée sur les récentes modifications de configuration jusqu'à ce que la session de redémarrage se déroule avec succès. Si la demande ne parvient pas à définir les attributs du BIOS, un message d'erreur s'affiche.

Supprimer toutes les valeurs en attente

Le bouton **Supprimer toutes les valeurs en attente** n'est actif que lorsque qu'il y a des valeurs en attente en raison des récentes modifications de configuration. Si l'utilisateur décide de ne pas appliquer les modifications de configuration, il peut cliquer sur **Supprimer**

toutes les valeurs en attente pour annuler toutes les modifications. Dans le cas où la demande ne parvient pas à supprimer les attributs du BIOS, un message d'erreur s'affiche.

Valeur en attente

La configuration d'un attribut du BIOS via iDRAC n'est pas appliquée immédiatement au BIOS. Le redémarrage du serveur est nécessaire pour que les modifications prennent effet. Lorsque vous modifiez un attribut du BIOS, la **valeur en attente** est mise à jour. Si un attribut a déjà une valeur en attente (et configurée), il s'affiche sur l'interface utilisateur.

Modification de la configuration du BIOS

La modification de la configuration du BIOS génère des entrées de journal d'audit qui sont enregistrées dans les journaux LC.

Analyse du BIOS en temps réel

L'analyse BIOS en temps réel vérifie l'intégrité et l'authenticité de l'image BIOS dans la mémoire ROM principale du BIOS lorsque l'hôte est sous tension mais pas dans l'auto-test de démarrage (POST).

REMARQUE :

- Cette fonctionnalité nécessite une licence iDRAC Datacenter.
- Vous devez disposer du privilège de débogage pour utiliser cette fonctionnalité.

L'iDRAC effectue automatiquement la vérification des sections immuables de l'image BIOS dans les scénarios suivants :

- Lors du cycle d'alimentation secteur/démarrage à froid
- Selon un planning défini par l'utilisateur
- À la demande (initiée par l'utilisateur)

Le résultat réussi de l'analyse en temps réel est enregistré dans le journal LC. Le résultat d'échec est enregistré dans les journaux LCL et SEL.

Sujets :

Analyse du BIOS en temps réel

L'analyse BIOS en temps réel vérifie l'intégrité et l'authenticité de l'image BIOS dans la mémoire ROM principale du BIOS lorsque l'hôte est sous tension mais pas dans l'auto-test de démarrage (POST).

REMARQUE :

- Cette fonctionnalité nécessite une licence iDRAC Datacenter.
- Vous devez disposer du privilège de débogage pour utiliser cette fonctionnalité.

iDRAC effectue automatiquement la vérification des sections immuables de l'image BIOS dans les scénarios suivants :

- Lors du cycle d'alimentation secteur/démarrage à froid
- Selon un planning défini par l'utilisateur
- À la demande (initiée par l'utilisateur)

Le résultat réussi de l'analyse en temps réel est enregistré dans le journal LC. Le résultat d'échec est enregistré dans les journaux LCL et SEL.

Récupération du BIOS et Root of Trust (RoT) du matériel

Pour le serveur PowerEdge, il est nécessaire d'effectuer une récupération à partir d'une image BIOS corrompue ou endommagée par des attaques malveillantes, des surtensions ou tout autre événement imprévisible. Une autre réserve d'image BIOS serait nécessaire pour récupérer le BIOS afin de faire rebasculer le serveur PowerEdge du mode fonctionnel sur le mode non amorçable. Ce BIOS alternatif ou de récupération est stocké dans un deuxième SPI (combiné au SPI BIOS principal).

La séquence de récupération peut être lancée via l'une des approches suivantes, iDRAC étant l'orchestrateur principal de la tâche de récupération du BIOS :

1. **Récupération automatique de l'image principale/de récupération du BIOS** : l'image BIOS est récupérée automatiquement au cours du processus de démarrage de l'hôte une fois la corruption du BIOS détectée par le BIOS lui-même.
2. **Récupération forcée de l'image principale/de récupération du BIOS** : l'utilisateur lance une demande OOB pour mettre à jour le BIOS, soit parce qu'il dispose d'un nouveau BIOS mis à jour, soit parce que le BIOS n'a pas pu s'amorcer.
3. **Mise à jour de la ROM principale du BIOS** : la ROM principale est divisée en ROM de données et ROM de code. L'iDRAC dispose d'un accès/contrôle total sur la ROM de code. Il commute MUX pour accéder à la mémoire ROM de code chaque fois que nécessaire.
4. **Root of Trust (RoT) du matériel BIOS** : cette fonctionnalité est disponible sur les serveurs portant le numéro de modèle RX5X, CX5XX et TX5X. Au cours de chaque amorçage de l'hôte (uniquement pour le démarrage à froid ou le cycle marche/arrêt, pas au cours du redémarrage à chaud), l'iDRAC s'assure que RoT est exécuté. RoT s'exécute automatiquement et l'utilisateur ne peut pas le lancer à l'aide d'une interface. Cette règle d'amorçage en premier d'iDRAC vérifie le contenu de la mémoire ROM du BIOS hôte à chaque cycle de marche/arrêt et chaque cycle CC hôte. Ce processus permet d'assurer un Secure Boot du BIOS et de sécuriser le processus de démarrage de l'hôte.

REMARQUE : Lors de la mise sous tension du serveur à partir de l'état **Hors tension**, il peut s'écouler entre 20 et 30 secondes pour que l'iDRAC affiche l'état d'alimentation **Sous tension**.

21

Configuration et utilisation de la console virtuelle

L'iDRAC dispose désormais d'une option HTML5 améliorée dans vConsole, qui active vKVM (clavier virtuel, vidéo et souris) sur le client VNC standard. Vous pouvez utiliser la console virtuelle pour gérer un système distant avec le clavier, la vidéo et la souris sur votre station de gestion, afin de contrôler les appareils correspondants sur un serveur géré. Il s'agit d'une fonctionnalité sous licence pour les serveurs rack et tour. Le privilège de configuration de l'iDRAC est nécessaire pour accéder à toutes les configurations de la console virtuelle.

Vous trouverez ci-dessous la liste des attributs configurables dans la console virtuelle :

- vConsole activée : Activée/Désactivée
- Sessions max. : 1 à 6
- Sessions actives : 0 à 6
- Chiffrement vidéo : Activé/Désactivé
- Vidéo locale du serveur : Activée/Désactivée
- Action dynamique sur le délai d'expiration de la demande de partage : Accès total, En lecture seule et Aucun accès
- Verrouillage automatique du système : Activé/Désactivé
- État de connexion du clavier/de la souris : Relier automatiquement, Relier et Détacher

Les principales fonctions sont les suivantes :

- Vous pouvez avoir jusqu'à six sessions de console virtuelle simultanées. Toutes les sessions affichent simultanément la même console de serveur géré.
- Vous pouvez lancer la console virtuelle dans un navigateur Web pris en charge.

  REMARQUE :
  - Toute modification apportée à la configuration de serveur Web entraînera la cessation de la session de la console virtuelle existante.
  - Même si l'option de chiffrement de la vidéo est désactivée dans l'interface utilisateur graphique, vous pouvez toujours configurer la fonctionnalité à l'aide d'autres interfaces. Le chiffrement vidéo est activé par défaut.
  - Le lien de la console virtuelle peut être interrompu lors de l'exécution de la contrainte vidéo dans Internet Explorer.
- 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 pouvez ouvrir jusqu'à 6 sessions de console virtuelle à partir de la station de gestion vers le serveur géré.
- Si un second utilisateur demande une session de console virtuelle, le premier utilisateur en est averti et a la possibilité de refuser l'accès, d'autoriser l'accès en lecture seule ou d'autoriser un accès partagé total. Le second utilisateur est averti qu'un autre utilisateur a le contrôle. Le premier utilisateur doit répondre dans les 30 secondes, sans quoi l'accès sera accordé au second utilisateur sur la base des paramètres par défaut. Si ni le premier, ni le second utilisateur ne dispose de droits d'administrateur, le fait de quitter la session du premier utilisateur mettra fin automatiquement à celle du second.
- Les journaux de démarrage et les journaux de blocage sont capturés sous forme de journaux vidéo au format MPEG1.
- L'écran de blocage est capturé sous forme de fichier JPEG.

.

REMARQUE : Le nombre de sessions de console virtuelle actives affichées dans l'interface Web ne concerne que les sessions actives d'interface Web. Ce nombre n'inclut pas les sessions d'autres interfaces comme SSH et RACADM.

REMARQUE : Pour plus d'informations sur la configuration de votre navigateur pour accéder à la console virtuelle, reportez-vous à la section Configuration des navigateurs Web pour utiliser la console virtuelle.

Sujets :

- Lancement de la console virtuelle
- Utilisation de Virtual Console Viewer

Résolutions d'écran prises en charge et taux de rafraîchissement correspondants

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 50. Résolutions d'écran prises en charge et taux de rafraîchissement correspondants

Résolution de l'écran	Taux d'actualisation (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60
1920x1200	60

Il est recommandé de configurer la résolution d'affichage de l'écran sur 1 920 x 1 200 pixels.

La console virtuelle prend en charge une résolution vidéo maximale de 1 920 x 1 200 à un taux d'actualisation de 60 Hz. Afin d'atteindre cette résolution, les conditions suivantes sont requises :

- KVM/écran connecté à un connecteur VGA prenant en charge une résolution de 1 920 x 1 200
- Dernier pilote vidéo Matrox en date (pour Windows)

Lorsqu'un écran/KVM local avec une résolution maximale inférieure à 1 920 x 1 200 est connecté à un connecteur VGA, la résolution maximale prise en charge par la console virtuelle est réduite.

La console virtuelle iDRAC utilise le contrôleur graphique Matrox G200 intégré pour déterminer la résolution maximale de l'écran connecté lorsqu'un affichage physique est présent. Lorsque l'écran prend en charge une résolution de 1 920 x 1 200 ou supérieure, la console virtuelle prend en charge une résolution de 1 920 x 1 200. Si l'écran connecté prend en charge une résolution maximale inférieure (comme de nombreux KVMS), la résolution maximale de la console virtuelle est limitée.

Résolutions maximales de la console virtuelle basées sur le ratio d'affichage de l'écran :

- Écran 16:10 : 1 920 x 1 200 de résolution maximale
- Écran 16:9 : 1 920 x 1 080 de résolution maximale

Lorsqu'un écran physique n'est pas connecté à un port VGA sur le serveur, le système d'exploitation installé détermine les résolutions disponibles pour la console virtuelle.

Résolutions maximales de la console virtuelle en fonction du système d'exploitation de l'hôte sans surveillance physique :

- Windows : 1 600 x 1 200 (1 600 x 1 200, 1 280 x 1 024, 1 152 x 864, 1 024 x 768, 800 x 600)
- Linux : 1 024 x 768 (1 024 x 768, 800 x 600, 848 x 480, 640 x 480)

REMARQUE : Si une résolution supérieure via la console virtuelle est requise en l'absence de KVM ou d'écran physique, vous pouvez utiliser un dongle d'émulateur d'affichage VGA pour imiter une connexion d'écran externe avec une résolution allant jusqu'à 1 920 x 1 080.

REMARQUE : Si vous avez une session de console virtuelle active et qu'un écran de 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 exécute un système d'exploitation Linux, il se peut qu'une console X11 ne soit pas visible sur le écran local. Appuyez sur <Ctrl><Alt><F1> sur la console virtuelle iDRAC pour basculer Linux vers une console texte.

Configuration d'une 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 iDRAC ou de l'interface de ligne de commande RACADM.

Configuration de la console virtuelle à l'aide de l'interface web

Pour configurer la console virtuelle à l'aide de l'interface web d'iDRAC :

1. Accédez à **Configuration** > **Console virtuelle**. Cliquez sur le lien **Démarrer la console virtuelle**. La page Console virtuelle s'affiche.
2. Activez la console virtuelle et indiquez les valeurs requises. Pour plus d'informations sur les options, voir l'**Aide en ligne d'iDRAC**.

   REMARQUE : Si vous utilisez le système d'exploitation Nano, désactivez le **verrouillage automatique du système** dans la page **Console virtuelle**.

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 la commande `set` avec les objets du groupe **iDRAC.VirtualConsole**.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Prévisualisation de la console virtuelle

Avant de lancer la console virtuelle, vous pouvez afficher un aperçu de son état sur la page **Système** > **Propriétés** > **Récapitulatif du système**. La section **Présentation de la console virtuelle** affiche une image montrant l'état de la console virtuelle. Cette image est actualisée toutes les 30 secondes. Il s'agit d'une fonctionnalité 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'iDRAC 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, assurez-vous que :

- Vous disposez des privilèges d'administrateur.
- Une bande passante minimale de 1 Mo/s est disponible.

REMARQUE : Lorsque le port HTTP personnalisé ou le port par défaut est configuré dans l'iDRAC, effacez le cache du navigateur, puis lancez l'iDRAC avec HTTPS et acceptez les certificats. Ensuite, connectez-vous à l'iDRAC et lancez la console virtuelle.

REMARQUE : Si le contrôleur vidéo intégré est désactivé dans le BIOS et que vous lancez la console virtuelle, le Virtual Console Viewer (visualiseur de la console virtuelle) sera vide.

La console virtuelle inclut les commandes de console suivantes :

1. **Général** : définit les macros de clavier, le format d'image et le mode tactile.
2. **KVM** : affiche les valeurs de la fréquence d'image, de la bande passante, de la compression et du taux de paquets.
3. **Performances** : modifie la qualité et la vitesse de la vidéo.
4. **Liste des utilisateurs** : affiche la liste des utilisateurs connectés à la console.

Vous pouvez accéder au média virtuel en cliquant sur l'option **Connecter un média virtuel** disponible dans la console virtuelle.

REMARQUE : Dans la version 5.10.00.00 de l'iDRAC, si la session RFS est active, la session de média virtuel est bloquée. Par conséquent, lorsque vous effectuez une mise à niveau de la version 4.40.00.00 vers la version 5.10.00.00 avec la session RFS active, RFS est remonté lorsque l'iDRAC est activé. Dans ce cas, si vous tentez de lancer la session de média virtuel, elle échoue avec le message d'erreur `Virtual media already in use`.

Lancement de la console virtuelle à l'aide de l'interface Web

Vous pouvez lancer la console virtuelle des manières suivantes :

- Accédez à **Configuration** > **Console virtuelle**. Cliquez sur le lien **Démarrer la console virtuelle**. La page Console virtuelle s'affiche.

Le **Visualiseur de console virtuelle** affiche le bureau du système distant. À l'aide de ce visualiseur, vous pouvez contrôler les fonctions du clavier et de la souris du système distant à partir de votre station de gestion.

Plusieurs messages peuvent s'afficher suite au lancement de l'application. Pour empêcher tout accès non autorisé à l'application, parcourez ces messages dans un délai de trois minutes. Vous serez sinon invité à relancer 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.

Lancement de la console virtuelle avec une 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://adresse IP_iDRAC/console**
2. La page **Ouverture de session** correspondante s'affiche en fonction de la configuration d'ouverture de session :
   - Si l'authentification unique 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 connexions locales, Active Directory, LDAP, par carte à puce et par authentification unique (SSO). Firefox prend en charge les connexions locales, AD et SSO sur les systèmes d'exploitation Windows et les connexions 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.

Utilisation de Virtual Console Viewer

Le Visualiseur de console virtuelle fournit diverses commandes telles que la synchronisation de la souris, l'évolution de la console virtuelle, les options de chat, les macros du clavier, les actions d'alimentation, les périphériques de démarrage suivants et l'accès au Média virtuel. Pour plus d'informations sur ces fonctionnalités, voir l'**aide en ligne de l'iDRAC**.

REMARQUE : Si le serveur distant est hors tension, le message « Aucun signal » s'affiche.

La barre de titre du visualiseur de console virtuelle affiche le nom DNS ou l'adresse IP de l'iDRAC auquel vous êtes connecté à partir de la station de gestion. Si l'iDRAC ne dispose pas d'un nom DNS, l'adresse IP s'affiche. Le format est :

- Pour les serveurs au format rack et les serveurs tours : `<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`

Parfois, le visualiseur de console virtuelle peut afficher une vidéo de faible qualité. Cela à la connectivité réseau trop lente, qui entraîne une perte d'une ou deux trames vidéo lorsque vous démarrez la session de console virtuelle. Pour transmettre toutes les trames vidéo et améliorer la qualité de la vidéo, effectuez l'une des opérations 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**.

Utilisation d'une console virtuelle

REMARQUE : Par défaut, le type de console virtuelle est défini sur eHTML5.

Vous pouvez lancer une console virtuelle en tant que fenêtre contextuelle à l'aide de l'une des méthodes suivantes :

- Sur la page d'accueil de l'iDRAC, cliquez sur le lien **Démarrer la console virtuelle** disponible dans la session Prévisualisation de la console.
- Sur la page Console virtuelle de l'iDRAC, cliquez sur le lien **Démarrer la console virtuelle**.
- Sur la page de connexion de l'iDRAC, saisissez **https//<iDRAC IP>/console**. Il s'agit de la méthode Direct Launch (Lancement direct).

Les options de menu suivantes sont disponibles dans la console virtuelle eHTML5 :

- Alimentation
- Boot (Amorçage)
- Tchat
- Clavier
- Capture d'écran
- Actualiser
- Plein écran
- Déconnecter le visualiseur
- Commandes de la console
- Support virtuel

L'option **Envoyer toutes les frappes au serveur** n'est pas prise en charge sur la console virtuelle eHTML5. Utilisez le clavier et les macros de clavier pour toutes les touches de fonction.

- **Général** :
  - **Commande de la console** : dispose des options de configuration suivantes :
    - Macros de clavier : elles sont prises en charge dans la console virtuelle eHTML5 et sont accessibles en tant qu'options dans les menus déroulants suivants. Cliquez sur **Appliquer** pour appliquer la touche sélectionnée sur le serveur.
      - Ctrl+Alt+Suppr
      - Ctrl +Alt + F1
      - Ctrl +Alt + F2
      - Ctrl +Alt + F3
      - Ctrl +Alt + F4
      - Ctrl +Alt + F5
      - Ctrl +Alt + F6
      - Ctrl +Alt + F7
      - Ctrl +Alt + F8
      - Ctrl +Alt + F9
      - Ctrl +Alt + F10
      - Ctrl +Alt + F11
      - Ctrl +Alt + F12
      - Alt+Tab
      - Alt+Échap
      - Ctrl+Échap
      - Alt+Espace
      - Alt+Entrée
      - Alt+Tiret
      - Alt + F1
      - Alt + F2
      - Alt + F3
      - Alt + F4
      - Alt + F5
      - Alt + F6
      - Alt + F7
      - Alt + F8
      - Alt + F9
      - Alt + F10
      - Alt + F11
      - Alt + F12
      - ImprÉcr
      - Alt+ImprÉcr
      - F1

- Suspendre
- Onglet
- Ctrl+Entrée
- SysRq
- Alt+SysRq
- Win-P

▪ Format d'image : la taille de l'image vidéo de la console virtuelle eHTML5 est automatiquement ajustée pour optimiser la visibilité. Les options de configuration suivantes s'affichent dans une liste déroulante :
- Maintenance
- Ne pas entretenir

Cliquez sur **Appliquer** pour appliquer les paramètres sélectionnés sur le serveur.

▪ Mode tactile : la console virtuelle eHTML5 prend en charge la fonctionnalité de mode tactile. Les options de configuration suivantes s'affichent dans une liste déroulante :
- Direct
- Relatif

Cliquez sur **Appliquer** pour appliquer les paramètres sélectionnés sur le serveur.

- **Presse-papiers virtuel** : le presse-papiers virtuel vous permet de couper/copier/coller de la mémoire tampon de texte à partir de la console virtuelle vers le serveur hôte de l'iDRAC. Le serveur hôte peut être le BIOS, UEFI ou une invite du système d'exploitation. Il s'agit d'une action unidirectionnelle à partir du système client vers le serveur hôte de l'iDRAC uniquement. Suivez les étapes ci-après pour utiliser le presse-papiers virtuel :
  - Placez le curseur de la souris ou le focus du clavier sur la fenêtre de votre choix dans le bureau du serveur hôte.
  - Sélectionnez le menu **Commandes de la console** à partir de vConsole.
  - Copiez la mémoire tampon du presse-papiers du système d'exploitation à l'aide des touches de raccourci clavier, de la souris ou des commandes du pavé tactile, en fonction du système d'exploitation client. Vous pouvez également saisir le texte manuellement dans la zone de texte.
  - Cliquez sur **Envoyer le presse-papiers à l'hôte**.
  - Le texte s'affiche ensuite dans la fenêtre active du serveur hôte.

  REMARQUE :
  - Cette fonctionnalité est disponible avec la licence Enterprise et Datacenter.
  - Cette fonctionnalité ne prend en charge que le texte ASCII.
  - Cette fonctionnalité prend uniquement en charge le clavier anglais.
  - Les caractères de contrôle ne sont pas pris en charge.
  - Des caractères tels que **Nouvelle ligne** et **Tabulation** sont autorisés.
  - La taille de la mémoire tampon du texte ne doit pas comporter plus de 4 000 caractères.
  - Si la taille de la mémoire tampon collée est supérieure à la valeur maximale, la zone d'édition de l'interface utilisateur de l'iDRAC la tronque à la taille maximale de la mémoire tampon.

- **KVM** : ce menu répertorie les composants en lecture seule suivants :
  - Fréquence d'images
  - Bande passante
  - Compression
  - Taux de paquets
- **Performances** : utilisez le curseur pour régler la **Qualité vidéo maximale** et la **Vitesse vidéo maximale**.
- **Liste d'utilisateurs** : affichez la liste des utilisateurs connectés à la console virtuelle.
- **Clavier** : le clavier virtuel modifie sa mise en page en fonction de la langue du navigateur, c'est ce qui le différencie du clavier physique.

  REMARQUE : Veillez à ce que la langue du clavier virtuel et la langue du système d'exploitation hôte soient identiques.

- **Média virtuel** : cliquez sur l'option **Connecter un média virtuel** pour démarrer la session de média virtuel.
  - **Connecter un média virtuel** : ce menu contient les options de mappage du CD/DVD, de mappage du disque amovible, de mappage des périphériques externes et de réinitialisation du périphérique USB.
  - **Statistiques du média virtuel** : ce menu affiche le taux de transfert (en lecture seule). En outre, il présente les informations relatives au CD/DVD et aux disques amovibles, tels que les informations de mappage, le statut (en lecture seule ou non), la durée et les octets en lecture/écriture.
  - **Créer une image** : ce menu vous permet de sélectionner un dossier local et de générer un fichier FolderName.img avec le contenu du dossier local.

REMARQUE : Pour des raisons de sécurité, l'accès en lecture/écriture est désactivé lorsque vous accédez à la console virtuelle dans eHTML5.

Navigateurs pris en charge

La console virtuelle eHTML5 est prise en charge sur les navigateurs suivants :

- Microsoft EDGE
- Safari 16.6
- Safari 17.x
- Mozilla Firefox 128
- Mozilla Firefox 129
- Mozilla Firefox 130
- Google Chrome 137
- Google Chrome 138

REMARQUE : Il est recommandé d'installer Mac OS version 10.10.2 (ou supérieure) sur le système.

REMARQUE : Si vous utilisez le navigateur Chrome/Edge, un message de refus de connexion peut s'afficher.

Pour plus de détails sur les navigateurs et les versions pris en charge, voir le document *Notes de mise à jour du guide de l'utilisateur d'Integrated Dell Remote Access Controller* disponibles sur la page des manuels iDRAC..

22

Utilisation de l'iDRAC Service Module

L'iDRAC Service Module est une application logicielle recommandée pour une installation sur le serveur (elle n'est pas installée par défaut). Ce module complète iDRAC avec les données de surveillance du système d'exploitation. Elle complète l'iDRAC en fournissant des données supplémentaires pour utiliser des interfaces iDRAC telles que l'interface Web, Redfish et RACADM. Vous pouvez configurer les fonctionnalités surveillées par l'iDRAC Service Module pour contrôler le processeur ainsi que la mémoire utilisée sur le système d'exploitation du serveur. L'interface de ligne de commande du système d'exploitation hôte a été introduite pour activer ou désactiver l'état du cycle d'alimentation complet de tous les composants du système, à l'exception du bloc d'alimentation.

REMARQUE :

- Utilisez l'iDRAC Service Module uniquement si vous avez installé une licence de contrôleur iDRAC Express ou iDRAC Enterprise/ Datacenter.
- Les versions de l'iSM antérieures à 4.2 ne prennent pas en charge TLS 1.3.
- Si le réseau hôte n'est pas configuré correctement, la page SupportAssist de l'iDRAC signale le journal LC indiquant un problème de connexion à l'iSM.
- Si l'avertissement SRV042 figure dans le journal LC de l'iDRAC lors de la création de collectes SupportAssist, effectuez une réinitialisation matérielle de l'iDRAC pour résoudre cet avertissement dans le journal LC de l'iDRAC.

Avant d'utiliser l'iDRAC Service Module, assurez-vous que :

- Vous disposez de privilèges de connexion, de configuration et de contrôle de serveur dans l'iDRAC pour activer ou désactiver les fonctions de l'iDRAC Service Module.
- Vous ne désactivez pas l'option **Configuration d'iDRAC à l'aide de l'interface locale RACADM**.
- Le canal de connexion directe entre le système d'exploitation et l'iDRAC est activé par l'intermédiaire du bus USB interne dans l'iDRAC.

REMARQUE : Si vous effectuez la suppression de LC, les valeurs `idrac.Servicemodule` peuvent toujours afficher les anciennes valeurs.

REMARQUE :

- Lors de la première exécution de l'iDRAC Service Module, le canal de connexion directe est par défaut activé entre le système d'exploitation et l'iDRAC dans l'iDRAC. Si vous désactivez cette fonction après l'installation de l'iDRAC Service Module, vous devez l'activer manuellement dans l'iDRAC.
- Si le canal de connexion directe entre le système d'exploitation et l'iDRAC est activé via le LOM dans l'iDRAC, vous ne pouvez pas utiliser l'iDRAC Service Module.

Sujets :

Installation de l'iDRAC Service Module

Vous pouvez télécharger et installer l'iDRAC Service Module depuis le site **dell.com/support**. Vous devez disposer de privilèges d'administration sur le système d'exploitation du serveur pour installer l'iDRAC Service Module (Module de service iDRAC). Pour plus d'informations sur l'installation, voir le guide de l'utilisateur de l'iDRAC Service Module disponible sur la page iDRAC Service Module.

REMARQUE : Si la carte réseau USB est désactivée sur l'iDRAC, le programme d'installation de l'iSM l'active automatiquement. Une fois l'installation terminée, désactivez la carte réseau USB si nécessaire.

Installation d'iDRAC Service Module à partir du contrôleur iDRAC Core

Dans la page de configuration de l'**iDRAC Service Module**, cliquez sur **Installer Service Module**.

1. Le programme d'installation de Service Module est disponible pour le système d'exploitation hôte et une tâche est créée dans l'iDRAC. Pour le système d'exploitation Microsoft Windows ou le système d'exploitation Linux, connectez-vous au serveur à distance ou localement.
2. Recherchez le volume monté appelé « **SMINST** » dans la liste des appareils, puis exécutez le script approprié :
   - Sous Windows, ouvrez l'invite de commande et exécutez le fichier de commandes **ISM-Win.bat**.
   - Sous Linux, ouvrez l'invite shell et exécutez le fichier de script **ISM-Lx.sh**.
3. Une fois l'installation terminée, l'iDRAC indique que le module de service est **installé** et affiche la date d'installation.

   REMARQUE : Le programme d'installation est disponible pour le système d'exploitation hôte durant 30 minutes. Si vous ne démarrez pas l'installation dans ce délai de 30 minutes, vous devez redémarrer l'installation de Service Module.

Installation d'iDRAC Service Module à partir du contrôleur iDRAC Enterprise

1. Dans l'interface utilisateur de l'iDRAC, accédez à **Paramètres iDRAC** > **Paramètres** > **Configuration d'iDRAC Service Module**.
2. Dans la page **Configuration du module de service iDRAC**, cliquez sur **Installer le module de service**.
3. Cliquez sur **Lancer la console virtuelle**, puis sur **Continuer** dans la boîte de dialogue Avertissement de sécurité.
4. Pour trouver le fichier du programme d'installation iSM, connectez-vous au serveur à distance ou localement.

   REMARQUE : Le programme d'installation est disponible pour le système d'exploitation hôte durant 30 minutes. Si vous ne lancez pas l'installation dans un délai de 30 minutes, vous devez relancer l'installation.

5. Recherchez le volume monté appelé « **SMINST** » dans la liste des appareils, puis exécutez le script approprié :
   - Sous Windows, ouvrez l'invite de commande et exécutez le fichier de commandes **ISM-Win.bat**.
   - Sous Linux, ouvrez l'invite shell et exécutez le fichier de script **ISM-Lx.sh**.
6. Suivez les instructions qui s'affichent pour terminer l'installation.
   Sur la page **Configuration d'iDRAC Service Module**, le bouton **Installer Service Module** est désactivé une fois l'installation terminée et que l'état de Service Module affiché est **En cours d'exécution**.

Systèmes d'exploitation pris en charge de l'iDRAC Service Module

Pour obtenir la liste des systèmes d'exploitation pris en charge par l'iDRAC Service Module, voir le guide de l'utilisateur de l'iDRAC Service Module disponible sur la page iDRAC Service Module.

Fonctionnalités de surveillance de l'iDRAC Service Module

L'iDRAC Service Module (iSM) offre les fonctionnalités de surveillance suivantes :

Tableau 51. Fonctionnalités iSM prises en charge

En cours d'exécution	En cours d'exécution (fonctionnalités limitées)
Prise en charge de profil Redfish pour les attributs réseau	Service sur le SE hôte
Réinitialisation matérielle de l'iDRAC	Informations sur le système d'exploitation

Tableau 51. Fonctionnalités iSM prises en charge (suite)

En cours d'exécution	En cours d'exécution (fonctionnalités limitées)
Accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte (fonctionnalité expérimentale)	Récupération automatique du système
Alertes SNMP intrabande de l'iDRAC	Autorisation du module de service à effectuer une réinitialisation matérielle de l'iDRAC
Affichage des informations sur le système d'exploitation	S/O
Réplication des journaux Lifecycle Controller dans les journaux du système d'exploitation.	S/O
Options de récupération automatique du système	S/O
Saisie des fournisseurs de gestion WMI (Windows Management Instrumentation)	S/O
Intégration à la collecte SupportAssist. **REMARQUE :** Cela s'applique uniquement si l'iDRAC Service Module version 2.0 ou supérieure est installé.	S/O
Préparation au retrait du périphérique SSD PCIe NVMe **REMARQUE :** Pour plus d'informations, voir la page Support pour Dell iDRAC Service Module.	S/O
Cycle de marche/arrêt du serveur distant	S/O

Prise en charge de profil Redfish pour les attributs réseau

L'iDRAC Service Module v2.3 ou ultérieure fournit à l'iDRAC des attributs réseau supplémentaires qui peuvent être obtenus via les clients REST à partir de l'iDRAC. Pour en savoir plus, voir Prise en charge de profil Redfish par l'iDRAC.

Réplication des journaux Lifecycle dans ceux de l'OS

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 l'interface équivalente RACADM) sont répliqués dans le journal du système d'exploitation à l'aide de l'iDRAC Service Module. 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.

L'iDRAC Service Module journalise également les événements qui se sont produits lorsque le système d'exploitation ne fonctionnait pas. La journalisation de l'OS effectuée par l'iDRAC Service Module respecte les normes Syslog IETF pour les systèmes d'exploitation Linux.

REMARQUE : Sous Microsoft Windows, si les événements iSM sont consignés dans les journaux du système au lieu des journaux d'applications, redémarrez le service Journal des événements Windows ou redémarrez le système d'exploitation de l'hôte.

Options de récupération automatique du système

La fonction de récupération automatique du système est un temporisateur basé sur le matériel. En cas de panne matérielle, une notification peut ne pas être disponible, mais le serveur est réinitialisé comme si l'interrupteur d'alimentation avait été activé. La récupération automatique du système est implémentée à l'aide d'un temporisateur au compte à rebours s'effectuant en continu. Le moniteur d'intégrité recharge fréquemment le compteur pour empêcher le compte à rebours d'arriver à zéro. Si cela arrivait, il serait supposé que le système d'exploitation est bloqué et que le système tente automatiquement de redémarrer l'ordinateur.

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 les doublons d'entrées de l'horloge de surveillance.

Prise en charge intrabande des alertes SNMP d'iDRAC

À l'aide de l'iDRAC Service Module v2.3, vous pouvez recevoir des alertes SNMP du système d'exploitation hôte similaires aux alertes générées par l'iDRAC.

Vous pouvez également surveiller les alertes SNMP d'iDRAC sans configurer l'iDRAC et gérer à distance le serveur en configurant les interruptions et destinations SNMP sur le système d'exploitation de l'hôte. Dans l'iDRAC Service Module v2.3 ou ultérieure, cette fonction convertit tous les journaux Lifecycle répliqués dans les journaux du système d'exploitation en interruptions SNMP.

REMARQUE : Cette fonction est active uniquement si la fonction de réplication des journaux Lifecycle est activée.

REMARQUE : Sur les systèmes d'exploitation Linux, cette fonction exige qu'un SNMP principal ou de système d'exploitation soit activé avec le protocole de multiplexage SNMP (SMUX).

Par défaut, cette fonctionnalité est désactivée. Bien que le mécanisme d'alerte SNMP intrabande peut coexister avec le mécanisme d'alerte SNMP de l'iDRAC, les journaux enregistrés peuvent présenter des alertes SNMP redondantes issues des deux sources. Il est recommandé d'utiliser l'option intrabande ou hors bande, mais pas les deux.

Utilisation des commandes

Cette section présente l'utilisation des commandes des systèmes d'exploitation Windows, Linux et ESXi.

- **Système d'exploitation Linux**
  - Sur tous les systèmes d'exploitation Linux pris en charge par iSM, iSM fournit une commande exécutable. Vous pouvez exécuter cette commande en vous connectant au système d'exploitation avec SSH ou un équivalent.
  - À partir d'iSM 2.4.0, la commande suivante vous permet de configurer Agent-x en tant que protocole par défaut pour les alertes SNMP iDRAC intrabande :

```
./Enable-iDRACSNMPTrap.sh 1/agentx –force
```

Si –force n'est pas spécifié, assurez-vous que le net-SNMP est configuré et redémarrez le service snmpd.

  - Pour activer cette fonction :

```
Enable-iDRACSNMPTrap.sh 1
```

```
Enable-iDRACSNMPTrap.sh enable
```

  - Pour désactiver cette fonction :

```
Enable-iDRACSNMPTrap.sh 0
```

```
Enable-iDRACSNMPTrap.sh disable
```

REMARQUE : L'option **--force** configure Net-SNMP pour transférer les interruptions. Vous devez cependant configurer la destination d'interruption.

- **Système d'exploitation VMware ESXi**

REMARQUE : Vous devez examiner et configurer les paramètres SNMP d'interruptions à l'échelle du système VMware ESXi.

REMARQUE : pour plus de détails, voir le livre blanc technique **Alertes SNMP intrabande** disponible sur la page de Support Dell.

l'accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte

En utilisant cette fonction, vous pouvez configurer et surveiller les paramètres matériels via l'interface Web de l'iDRAC et RedFish, à l'aide de l'adresse IP de l'hôte sans configurer l'adresse IP de l'iDRAC. Vous pouvez utiliser les informations d'identification iDRAC par défaut si le serveur iDRAC n'est pas configuré ou continuer à utiliser les mêmes informations d'identification si le serveur iDRAC a été configuré précédemment.

Accès à iDRAC via les systèmes d'exploitation Windows

Vous pouvez effectuer cette tâche à l'aide des méthodes suivantes :

- Installer la fonction d'accès à iDRAC à l'aide de webpack.

- Configurez le système avec un script iSM PowerShell.

Installation à l'aide de MSI

Vous pouvez installer cette fonction à l'aide du pack Web. Cette fonction est désactivée sur une installation iSM classique. Si cette option est activée, le numéro de port d'écoute par défaut est 1266. Vous pouvez modifier ce numéro de port compris entre 1024 et 65535. L'iSM redirige la connexion vers l'iDRAC. L'iSM crée ensuite une règle de pare-feu entrante, OS2iDRAC. Le numéro de port d'écoute est ajouté à la règle de pare-feu OS2iDRAC dans le système d'exploitation hôte, ce qui autorise les connexions entrantes. La règle de pare-feu est activée automatiquement lorsque cette fonction est activée.

À partir d'iSM 2.4.0, vous pouvez récupérer l'état actuel et la configuration du port d'écoute en utilisant la cmdlet PowerShell suivante :

```
Enable-iDRACAccessHostRoute -status get
```

La sortie de cette commande indique si cette fonction est activée ou désactivée. Si la fonction est activée, elle affiche le numéro de port d'écoute.

REMARQUE : Pour que cette fonction fonctionne, assurez-vous que le service d'assistance IP Microsoft est en cours d'exécution sur votre système .

Pour accéder à l'interface Web d'iDRAC, utilisez le format `https://<host-name>` ou `OS-IP>:443/login.html` dans le navigateur, où :

- `<host-name>` est le nom de l'hôte complet du serveur sur lequel iSM est installé et configuré pour l'accès à iDRAC via la fonctionnalité du système d'exploitation. Vous pouvez utiliser l'adresse IP du système d'exploitation si le nom de l'hôte n'est pas présent.
- `443` est la valeur par défaut du numéro de port de l'iDRAC. C'est ce que l'on appelle le numéro de port de connexion vers lequel toutes les connexions entrantes sur le numéro de port d'écoute sont redirigées. Vous pouvez modifier le numéro de port via l'interface Web de l'iDRAC, et des interfaces RACADM.

Configuration à l'aide d'une cmdlet PowerShell iSM

Si cette fonction est désactivée lors de l'installation d'iSM, vous pouvez activer la fonction à l'aide de la commande Windows PowerShell suivante fournie par iSM :

```
Enable-iDRACAccessHostRoute
```

Si la fonction est déjà configurée, vous pouvez la désactiver ou la modifier à l'aide de la commande PowerShell et des options correspondantes. Les options utilisables sont les suivantes :

- **Status** : ce paramètre est obligatoire. Les valeurs ne sont pas sensibles à la casse et la valeur peut être **true**, **false** ou **get**.
- **Port** : il s'agit du numéro de port d'écoute. Si vous n'indiquez pas de numéro de port, le numéro de port par défaut (1266) est utilisé. Si la valeur du paramètre **Status** est FALSE, vous pouvez ignorer le reste des paramètres. Vous devez saisir un nouveau numéro de port qui n'est pas déjà configuré pour cette fonction. Les nouveaux paramètres de numéro de port écrasent la règle de pare-feu entrante OS2iDRAC et vous pouvez utiliser le nouveau numéro de port pour vous connecter à l'iDRAC. La plage de valeurs est comprise entre 1024 et 65535.
- **IPRange** : ce paramètre est facultatif et il fournit une plage d'adresses IP qui sont autorisées à se connecter à l'iDRAC via le système d'exploitation hôte. Le format de la plage d'adresses IP est le format du routage interdomaine (CIDR) qui est une combinaison d'adresse IP et de masque de sous-réseau. Par exemple, 10.94.111.21/24. L'accès à iDRAC est restreint pour les adresses IP qui ne sont pas comprises dans la plage.

REMARQUE : Cette fonction ne prend en charge que les adresses IPv4.

Accès à iDRAC via les systèmes d'exploitation Linux

Vous pouvez installer cette fonctionnalité à l'aide du fichier `setup.sh`, disponible avec le pack Web. Cette fonction est désactivée par défaut sur une installation iSM classique. Pour consulter l'état de cette fonctionnalité, utilisez la commande suivante :

Pour installer, activer et configurer cette fonctionnalité, utilisez la commande suivante :

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0

Désactiver

`<source-port>` et `<source-IP-range/source-ip-range-mask>` ne sont pas requis.

<Enable-Flag>=1

Activer

`<source-port>` est requis et `<source-ip-range-mask>` est facultatif.

<source-IP-range>

Plage d'adresses IP au format **<adresse IP/masque sous-réseau>**. Exemple : 10.95.146.98/24

Utilisation de l'iDRAC Service Module à partir de l'interface Web iDRAC

Pour utiliser l'iDRAC Service Module à partir de l'interface Web iDRAC :

1. Accédez à **Paramètres iDRAC** > **Présentation** > **Module des services des iDRAC** > **Configurer les modules des services**. La page **Configuration de l'iDRAC Service Module** s'affiche.
2. Vous pouvez afficher ce qui suit :
   - La version de l'iDRAC Service Module installée sur le système d'exploitation hôte
   - L'état de connexion de l'iDRAC Service Module à l'iDRAC.

   REMARQUE : Lorsqu'un serveur a plusieurs systèmes d'exploitation et que l'iDRAC Service Module est installé sur tous les systèmes d'exploitation, l'iDRAC se connecte uniquement à l'instance la plus récente d'iSM parmi tous les systèmes d'exploitation. Une erreur s'affiche pour toutes les anciennes instances d'iSM sur les autres systèmes d'exploitation. Pour connecter iSM à l'iDRAC sur un autre système d'exploitation sur lequel iSM est déjà installé, désinstallez et réinstallez iSM sur ce système d'exploitation particulier.
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.
   - **Informations WMI** : inclut des informations sur WMI.
   - **Action de récupération de système automatique** : exécution des opérations de récupération automatique sur le système après un certain temps (en secondes) :
     - **Redémarrage**
     - **Arrêter le système**
     - **Cycle d'alimentation du système**

     Cette option est désactivée si OpenManage Server Administrator est installé sur le système.

REMARQUE : Lorsque l'iSM est dans un état de fonctionnalité de mode complet ou limité et que l'iDRAC est réinitialisé aux paramètres par défaut, il n'y a aucun moyen pour l'iDRAC de définir l'état de fonctionnalité du mode limité pour l'état iSM.

Utilisation de l'iDRAC Service Module à l'aide de RACADM

Pour utiliser l'iDRAC Service Module à partir de RACADM, utilisez les objets du groupe `ServiceModule`.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

23

Utilisation d'un port USB type-C Dual-mode pour la gestion du serveur

Sur les serveurs de 17e génération, un port USB type-C Dual-mode dédié est fourni dans le panneau de configuration, qui se trouve à l'avant du serveur. Par défaut, le port est en mode système d'exploitation. Un bouton ID du système (¡) se trouve sur le panneau de commande. Pour passer le port en mode iDRAC, appuyez sur le bouton ¡ et maintenez-le enfoncé pendant 5 à 10 secondes jusqu'à ce que le voyant LED de la clé à molette s'allume. Pour rétablir le mode système d'exploitation du port, appuyez de nouveau sur le bouton ¡ et maintenez-le enfoncé pendant 5 à 10 secondes, jusqu'à ce que le voyant LED de la clé à molette s'éteigne.

Les opérations d'importation de profils de configuration de serveur (SCP) via USB sont prises en charge uniquement avec une licence Enterprise ou Datacenter.

Vous pouvez exécuter les fonctions suivantes à l'aide du port USB type-C Dual-mode lorsque le port est en mode iDRAC :

- Connectez-vous au système à l'aide de l'interface réseau USB pour accéder aux outils de gestion des systèmes tels que l'interface Web iDRAC et RACADM.
- Configurez un serveur à l'aide des fichiers SCP qui sont stockés sur un lecteur USB.

REMARQUE : Pour gérer un port USB Type-C bi-mode ou configurer un serveur en important les fichiers de profil de configuration de serveur (SCP) sur un lecteur USB, vous devez disposer du privilège de Contrôle du système.

REMARQUE : Une alerte est générée lorsqu'un périphérique USB est inséré.

Sujets :

Configuration de l'iDRAC à l'aide du profil de configuration de serveur sur un périphérique USB

Avec le port USB type-C Dual-mode en mode iDRAC, vous pouvez configurer l'iDRAC sur le serveur. Configurez les paramètres de port bi-mode USB Type-C dans l'iDRAC, insérez le périphérique USB contenant le profil de configuration du serveur, puis importez le profil de configuration du serveur depuis le périphérique USB dans l'iDRAC.

Configuration des paramètres du port USB type-C Dual-mode à l'aide de l'interface utilisateur iDRAC

Pour configurer le port USB type-C Dual-mode :

1. Activez le port USB type-C Dual-mode du serveur dans l'iDRAC (**Configuration** > **Paramètres du BIOS** > **Périphériques intégrés**. Assurez-vous que l'option **Tous les ports activés** ou **Tous les ports désactivés (dynamique)** est définie sur **Ports USB accessibles par l'utilisateur**. Lorsque **Désactivation de tous les ports (Dynamique)** est sélectionné, assurez-vous que **Activer les ports avant uniquement** est **Activé**.
2. Appuyez sur le bouton ID du système sur le panneau de commande et maintenez-le enfoncé pendant environ 5 à 10 secondes jusqu'à ce que la LED de la clé s'allume.
   Le voyant LED USB devient vert fixe et le port est configuré en tant que port iDRAC.
3. Dans l'interface Web d'iDRAC, accédez à **Paramètres iDRAC** > **Paramètres** > **Paramètres de gestion USB**. Le **port de gestion USB** est défini sur **Activé**.
4. À partir de **Géré par l'iDRAC : USB SCP**, sélectionnez l'une des options activées :
   - **Désactivé**
   - **Activé uniquement lorsque le serveur est doté de paramètres de références par défaut**
   - **Activé uniquement pour les fichiers de configuration compressés**

- **Activé**

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

REMARQUE : iDRAC10 vous permet de protéger le fichier compressé par mot de passe après que vous avez sélectionné Activé uniquement pour les fichiers de configuration compressés afin de compresser le fichier avant de l'importer. Vous pouvez entrer un mot de passe pour sécuriser le fichier à l'aide de l'option Mot de passe du fichier zip.

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

Accès à l'interface iDRAC via connexion USB directe

La fonction iDRAC Direct vous permet de connecter directement votre ordinateur portable au port USB de l'iDRAC. Cette fonction vous permet d'interagir directement avec les interfaces iDRAC, telles que l'interface Web, RACADM et Redfish pour une gestion et une maintenance avancées des serveurs.

Pour consulter la liste des navigateurs et systèmes d'exploitation pris en charge, voir la *Notes de mise à jour du guide de l'utilisateur d'Integrated Dell Remote Access Controller* disponibles sur la page des manuels iDRAC..

REMARQUE : Si vous utilisez un système d'exploitation Windows, installez un pilote RNDIS pour pouvoir utiliser cette fonctionnalité.

Pour accéder à l'interface iDRAC via le port USB :

1. Éteignez tous les réseaux sans fil et déconnectez-vous de tout autre réseau câblé. Assurez-vous qu'aucun des réseaux ou paramètres externes ou internes n'interfère avec la communication.
2. Assurez-vous que le port USB est en mode iDRAC.
3. Attendez quelques secondes que l'ordinateur portable acquière l'adresse IP 169.254.0.4. L'iDRAC acquiert l'adresse IP 169.254.0.3.
4. Commencez à utiliser les interfaces réseau iDRAC, comme l'interface Web, RACADM et Redfish.
   Par exemple, pour accéder à l'interface Web de l'iDRAC, ouvrez un navigateur pris en charge, saisissez l'adresse **169.254.0.3**, puis appuyez sur la touche <Entrée>.
5. Lorsque iDRAC utilise le port USB, le voyant clignote pour indiquer une activité. Le voyant clignote une fois toutes les deux secondes.
6. Une fois les actions requises effectuées, débranchez le câble USB du système.
   La LED revient au vert fixe.

Importation du profil de configuration du serveur depuis un périphérique USB

Créez un répertoire à la racine du périphérique USB appelé `System_Configuration_XML` qui contient les fichiers de configuration et de contrôle :

- Le profil de configuration du serveur (SCP) se trouve dans le sous-répertoire `System_Configuration_XML`, sous le répertoire racine du périphérique USB. Ce fichier contient toutes les paires attribut/valeur du serveur. Il inclut des attributs de l'iDRAC, PERC, RAID et BIOS. Vous pouvez modifier ce fichier pour configurer un attribut du serveur. Le nom du fichier peut être `<servicetag>-config.xml`, `<servicetag>-config.json`, `<modelnumber>-config.xml`, `<modelnumber>-config.json`, `config.xml` ou `config.json`.
- Fichier de contrôle : comprend les paramètres permettant de contrôler l'opération d'importation et ne possède pas les attributs de l'iDRAC ou d'un autre composant du système. Le fichier de contrôle contient trois paramètres :
  - ShutdownType : Normal, Forcé, Ne pas redémarrer.
  - TimeToWait (en secondes) : 300 minimum et 3 600 maximum.
  - EndHostPowerState : activé ou désactivé.

Exemple de fichier `control.xml` :

```
<InstructionTable>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>ShutdownType</Instruction>
     <Value>NoReboot</Value>
     <ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
```

```
      </InstructionType>
      <Instruction>TimeToWait</Instruction>
      <Value>300</Value>
      <ValuePossibilities>Minimum value is 300 -Maximum value is
       3600 seconds.</ValuePossibilities>
   </InstructionRow>
   <InstructionRow>
      <InstructionType>Configuration XML import Host control Instruction
      </InstructionType>
      <Instruction>EndHostPowerState</Instruction>
      <Value>On</Value>
      <ValuePossibilities>On,Off</ValuePossibilities>
   </InstructionRow>
</InstructionTable>
```

Vous devez disposer des privilèges de contrôle du serveur pour effectuer cette opération.

REMARQUE : Lors de l'importation du SCP, la modification des paramètres de gestion de l'USB dans le fichier SCP entraîne une tâche qui a échoué ou une tâche qui s'est terminée avec des erreurs. Vous pouvez commenter les attributs dans le SCP afin d'éviter des erreurs.

Pour importer le profil de configuration de serveur du périphérique USB à l'iDRAC :

1. Configurez le port de gestion USB :
   - Définissez le **Mode de port de gestion USB** sur **iDRAC**.
   - Définissez **iDRAC géré : SCP USB sur Activé avec les références par défaut** ou **Activé**.
2. Insérez la clé USB (qui contient le fichier `configuration.xml` et le fichier `control.xml`) dans le port USB de l'iDRAC.

   REMARQUE : Le nom et le type de fichier sont sensibles à la casse pour les fichiers XML. Assurez-vous que les deux sont en minuscules.

   REMARQUE : La clé USB doit disposer uniquement du système de fichiers FAT32 pris en charge.
3. Le profil de configuration du serveur est détecté sur le périphérique USB dans le sous-répertoire `System_Configuration_XML`, sous le répertoire racine du périphérique USB. Il est détecté dans la séquence suivante :
   - `<servicetag>-config.xml` / `<servicetag>-config.json`
   - `<modelnum>-config.xml` / `<modelnum>-config.json`
   - `config.xml` / `config.json`
4. Une tâche d'importation de profil de configuration de serveur démarre.

   Si le profil n'est pas détecté, l'opération s'arrête.

   Si l'option **iDRAC géré : configuration SCP USB** a été définie sur **Activé avec les références par défaut** et le mot de passe de configuration du BIOS n'a pas la valeur Null ou si l'un des comptes d'utilisateur iDRAC a été modifié, un message d'erreur s'affiche et l'opération s'arrête.
5. , le cas échéant, indiquent qu'une tâche d'importation a démarré.
6. Si une configuration doit être préparée et que le **type d'arrêt** est spécifié comme **Pas de redémarrage** dans le fichier de contrôle, redémarrez le serveur pour configurer les paramètres. Sinon, le serveur est redémarré et la configuration est appliquée. C'est uniquement lorsque le serveur est déjà hors tension que la configuration préparée s'applique même si l'option **Pas de redémarrage** est spécifiée.
7. Une fois la tâche d'importation terminée, le voyant LED indique que la tâche est terminée.
8. Si le périphérique USB reste inséré sur le serveur, le résultat de l'opération d'importation est enregistré dans le fichier `results.xml` du périphérique USB.

Journaux LC et messages d'erreur lors des opérations liées à l'USB

Lorsqu'un périphérique USB est connecté, la page **Inventaire du système** affiche les informations sur le périphérique USB sous la section Inventaire du matériel.

Un événement est journalisé dans les journaux Lifecycle Controller dans les cas suivants :

- Le périphérique est en mode iDRAC et le périphérique USB est inséré ou retiré.
- Le Mode Port de gestion USB est modifié.
- L'appareil passe manuellement du mode iDRAC au mode système d'exploitation.

- L'appareil est supprimé de l'iDRAC.

Lorsqu'un périphérique dépasse ses besoins en alimentation, comme autorisé par les spécifications USB, le périphérique est déconnecté et un événement de surtension est généré avec les propriétés suivantes :

- Catégorie : Intégrité du système
- Type : Périphérique USB
- Gravité : Avertissement
- Notifications autorisées : e-mail, trap SNMP et syslog distant
- Actions : Aucune

Un message d'erreur s'affiche et est consigné dans le journal du Lifecycle Controller dans les cas suivants :

- Lorsque les fichiers d'entrée pour l'opération du profil de configuration du serveur (SCP) sont incorrects.
- Lorsque le lecteur USB présente des erreurs matérielles ou des systèmes de fichiers non pris en charge.

Comportement du voyant LED

Le voyant LED USB indique l'état de fonctionnement d'un profil de configuration serveur en cours d'exécution par le port USB. Le voyant LED peut ne pas être disponible sur tous les systèmes.

- Éteint : le port USB type-C Dual-mode est en mode système d'exploitation.
- Vert fixe : le port USB est connectée à l'iDRAC ou le travail d'importation SCP a été réalisé avec succès.
- Vert clignotant : la tâche d'importation SCP ou les activités d'E/S sont en cours.
- Orange fixe : la tâche d'importation SCP a échoué.
- Orange clignotant : le matériel USB présente des erreurs.

Journaux et fichier de résultats

Les informations suivantes sont journalisées pour l'opération d'importation :

- L'importation automatique à partir de l'USB est journalisée dans le fichier journal du Lifecycle Controller.
- Si le périphérique USB reste inséré, les résultats de la tâche sont journalisés dans le fichier de résultats se trouvant sur la clé USB.

Un fichier de résultats appelé `Results.xml` est mis à jour ou créé dans le sous-répertoire avec les informations suivantes :

- Étiquette de service : les données sont enregistrées suite au renvoi d'un ID de tâche ou d'une erreur de l'opération d'importation.
- ID de tâche : les données sont enregistrées suite au renvoi d'un ID de tâche de l'opération d'importation.
- Date et heure de début de la tâche : les données sont enregistrées suite au renvoi d'un ID de tâche de l'opération d'importation.
- État : les données sont enregistrées suite au renvoi d'une erreur de l'opération d'importation ou lorsque les résultats de la tâche sont disponibles.

24

Utilisation de Quick Sync 2

Avec Dell OpenManage Mobile s'exécutant sur un appareil mobile Android ou iOS, vous pouvez facilement accéder au serveur directement ou via la console OpenManage Essentials ou OpenManage Enterprise (OME). Vous pouvez ainsi examiner les détails de serveur et l'inventaire, afficher les journaux d'événements système et LC, recevoir les notifications automatiques sur un appareil mobile à partir d'une console OME, affecter l'adresse IP et modifier le mot de passe iDRAC, configurer les attributs BIOS importants et entreprendre des mesures correctives selon vos besoins. Vous pouvez également effectuer un cycle de marche/arrêt d'un serveur, accéder à la console système ou accéder à l'interface graphique de l'iDRAC.

OMM peut être téléchargé gratuitement à partir d'Apple App Store ou de Google Play Store.

Vous devez installer l'application OpenManage Mobile sur l'appareil mobile Android (prend en charge les appareils mobiles Android 5.0 et versions ultérieures et iOS 9.0 et versions ultérieures) pour gérer le serveur à l'aide de l'interface Quick Sync 2 d'iDRAC.

REMARQUE : Cette section s'affiche uniquement pour les serveurs qui disposent du module Quick Sync 2 dans l'oreille gauche du rack.

REMARQUE : Cette fonctionnalité est actuellement prise en charge sur les appareils mobiles dotés du système d'exploitation Android et d'Apple iOS.

Une fois la configuration de Quick Sync terminée, activez le bouton Quick Sync 2 sur le panneau de commande gauche. Assurez-vous que le voyant Quick Sync 2 s'allume. Accédez aux informations Quick Sync 2 via un appareil mobile (Android 5.0 ou version ultérieure, iOS 9.0 ou version ultérieure, OMM 2.0 ou version ultérieure).

À l'aide d'OpenManage Mobile, vous pouvez :

- Afficher les informations sur l'inventaire
- Afficher les informations de surveillance
- Configurer les paramètres réseau iDRAC de base

Pour plus d'informations sur OpenManage Mobile, voir le *Guide de l'utilisateur de Dell OpenManage Mobile* disponible sur la page des manuels OpenManage..

Sujets :

Configuration d'iDRAC Quick Sync 2

À l'aide de l'interface Web de l'iDRAC, RACADM et iDRAC HII, vous pouvez configurer la fonctionnalité Quick Sync 2 de l'iDRAC pour autoriser l'accès à l'appareil mobile :

- **Accès** : définir sur lecture-écriture, lecture seule, et désactivé. Lecture-écriture est l'option par défaut.
- **Délai d'expiration** : définir sur activé ou désactivé. Activé est l'option par défaut.
- **Limite du délai d'expiration :** indique une durée au bout de laquelle le mode Quick Sync 2 est désactivé. Par défaut, l'option Minutes est sélectionnée. La valeur par défaut est 2 minutes. La plage va de 2 à 60 minutes.
  1. Si l'option est désactivée, vous pouvez spécifier une durée au bout de laquelle le mode Quick Sync 2 est désactivé. Pour activer, appuyez à nouveau sur le bouton d'activation.
  2. Si cette option est désactivée, l'horloge ne vous permet pas de spécifier une valeur d'expiration.
- **Authentification de lecture** : par défaut, cette option est activée.
- **WiFi** : par défaut, cette option est réglée sur Activé.

Vous devez disposer des privilèges de contrôle du serveur pour configurer ces paramètres. Le redémarrage du serveur n'est pas nécessaire pour que les paramètres prennent effet. Une fois la configuration terminée, vous pouvez activer le bouton Quick Sync 2 sur le panneau de configuration de gauche. Assurez-vous que le voyant Quick Sync s'allume. Ensuite, accédez aux informations Quick Sync via un appareil mobile.

Une entrée est consignée dans le journal du Lifecycle Controller lorsque la configuration est modifiée.

Configuration des paramètres de Quick Sync 2 de l'iDRAC à l'aide de RACADM

Pour configurer la fonction Quick Sync 2 de l'iDRAC, utilisez les objets RACADM du groupe **System.QuickSync**. Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Configuration des paramètres de la fonction iDRAC Quick Sync 2 à l'aide de l'interface Web

Pour configurer la fonction iDRAC Quick Sync 2 :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **iDRAC Quick Sync**.
2. Dans la section **iDRAC Quick Sync**, cliquez sur le menu déroulant **Accès**, puis sélectionnez l'une des options suivantes pour fournir un accès à l'appareil mobile Android ou iOS :
   - Lecture-écriture
   - Read-only (lecture seule)
   - Désactivé
3. Activez le temporisateur.
4. Spécifiez la limite du délai d'expiration.

   Pour plus d'informations sur les champs, voir l'**Aide en ligne de l'iDRAC**.
5. Cliquez sur **Appliquer** pour appliquer les paramètres.

Configuration des paramètres de la fonction iDRAC Quick Sync 2 à l'aide de l'utilitaire de configuration de l'iDRAC

Pour configurer la fonction iDRAC Quick Sync 2 :

1. Dans l'interface utilisateur graphique de l'iDRAC, accédez à **Configuration** > **Paramètres système** > **Paramètres matériels** > **iDRAC Quick Sync**.
2. Dans la section **Quick Sync iDRAC** :
   - Spécifiez le niveau d'accès.
   - Activez le délai d'expiration.
   - Renseignez le champ Limite du délai d'expiration défini par l'utilisateur (120 secondes à 3 600 secondes).

   Pour plus d'informations sur les champs, voir l'**Aide en ligne de l'iDRAC**.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres sont appliqués.

Utilisation d'un appareil mobile pour afficher des informations sur iDRAC

Pour afficher des informations sur l'iDRAC depuis un appareil mobile, voir le *Guide de l'utilisateur de Dell OpenManage Mobile* disponible sur la page des manuels OpenManage. pour connaître les étapes à suivre.

25

Gestion du média virtuel

L'iDRAC fournit le support virtuel avec un client basé sur HTML5 avec la prise en charge des fichiers ISO et IMG locaux, ISO et fichier IMG distants. 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. Vous devez disposer du privilège de configuration de l'iDRAC pour modifier la configuration.

Vous trouverez ci-dessous les attributs configurables :

- Média connecté activé : Activé ou Désactivé
- Mode de connexion : Relier automatiquement, Relier et Détacher
- Nombre maximal de sessions : 1
- Sessions actives : 1
- Chiffrement des médias virtuels : Activé (par défaut)
- Émulation de disquette : Désactivée (par défaut)
- Démarrer une seule fois : Activé ou Désactivé
- État de la connexion : Connecté ou Déconnecté

Avec la fonctionnalité Média Virtuel, vous pouvez :

- D'accéder à distance aux supports connectés à un système distant sur le réseau
- Installez les applications.
- De mettre à jour des pilotes
- Installez un système d'exploitation sur le système géré.

Les principales fonctions sont les suivantes :

- Le média virtuel prend en charge les lecteurs optiques virtuels (CD/DVD) et les clés USB.
- Vous pouvez connecter une seule clé USB, image ou clé et un seul lecteur optique à un système géré dans la station de gestion. 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.
- 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 de lecteur.
- 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 (en 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.

Après avoir joint une image de média virtuel à l'aide de la console virtuelle, il se peut que le disque ne s'affiche pas dans le système d'exploitation Windows hôte. Vérifiez le gestionnaire de périphériques Windows pour tous les périphériques de stockage de masse inconnus. Cliquez avec le bouton droit de la souris sur le périphérique inconnu et mettez à jour le pilote ou désinstallez le pilote. Le périphérique est reconnu par Windows après déconnexion et reconnexion du vMedia.

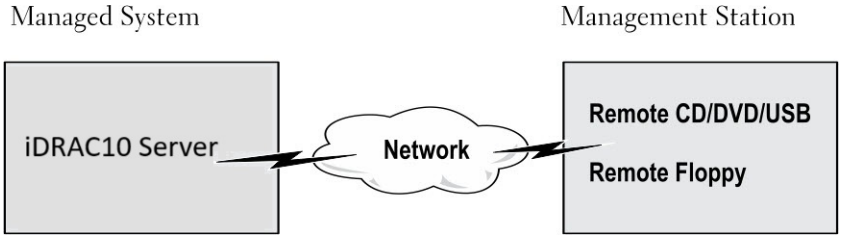


Figure 4. Configuration Média Virtuel

Sujets :

Lecteur et périphériques pris en charge

Le tableau suivant répertorie les lecteurs pris en charge via Média Virtuel.

Tableau 52. Lecteur et périphériques pris en charge

Disque	Support de stockage compatible
Lecteurs optiques virtuels	• Fichier image ISO • Fichier image IMG
Lecteurs Flash USB	• Fichier image USB au format ISO9660

Configuration de média virtuel

Configuration de média virtuel à l'aide de l'interface Web d'iDRAC

Pour définir les paramètres Média Virtuel :

PRÉCAUTION : Ne réinitialisez pas l'iDRAC lors de l'exécution d'une session de média virtuel. Dans le cas contraire, des résultats indésirables peuvent se produire, notamment une perte de données.

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Média virtuel** > **Média connecté**.
2. Indiquez le paramétrage requis. Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration de média virtuel à l'aide de RACADM

Pour configurer le média virtuel, utilisez la commande `set` avec les objets du groupe **iDRAC.VirtualMedia**.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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 de l'iDRAC. Pour ce faire, procédez comme suit :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Paramètres de port USB et média**.
   La page **Paramètres de port USB et de média de configuration d'iDRAC** s'affiche.
2. Dans la section **Média virtuel**, sélectionnez **Déconnecter**, **Connecter** ou **Connecter automatiquement** en fonction de vos besoins. Pour plus d'informations sur ces options, voir l'**Aide en ligne de l'utilitaire de configuration de l'iDRAC**.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres du média virtuel sont configurés.

État de média connecté et réponse du système

Le tableau suivant indique la réponse du système en fonction du paramètre Média connecté.

Tableau 53. État de média connecté et réponse du système

État de média connecté	Réponse du système
Détacher	Impossible de mapper une image au système.
Attacher	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.

Paramètres du serveur pour l'affichage des périphériques virtuels dans Virtual Media

Vous devez configurer les paramètres suivants dans la station de gestion pour activer la visibilité des lecteurs vides. Pour ce faire, ouvrez l'Explorateur Windows, accédez au menu **Organiser**, puis cliquez sur **Options des dossiers et de recherche**. Dans l'onglet **Affichage**, désélectionnez l'option **Masquer les lecteurs vides dans le dossier Ordinateur**, puis cliquez sur **OK**.

Accès à un média virtuel

Vous pouvez accéder au Média virtuel avec ou sans la console virtuelle. Avant d'accéder au Média virtuel, veillez à configurer votre ou vos navigateurs Web.

Les fonctionnalités de Média virtuel et RFS s'excluent mutuellement. 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 n'est actuellement pas disponible. Une session Média virtuel ou une session RFS est en cours**.

Les fonctionnalités de Média virtuel et RFS s'excluent mutuellement. Si la connexion RFS n'est pas active et que vous tentez de lancer le client Média virtuel, le message d'erreur suivant s'affiche : `Virtual Media is currently unavailable. A Virtual Media or Remote File Share session is in use. If virtual media connected first then user can able to connect RFS1 also.`

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 de Média virtuel.

Le fichier.img mappé via **Console virtuelle** > **Média virtuel ou Média virtuel autonome** ne prend pas en charge les opérations d'écriture dans le système d'exploitation hôte.

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 de l'iDRAC, accédez à **Configuration** > **Console virtuelle**.
   La page **Console virtuelle** s'affiche.
2. Cliquez sur **Lancer la console virtuelle**.
   Le **Visualiseur de console virtuelle** s'ouvre.
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.

Lancement de Média Virtuel sans utiliser la console virtuelle

Avant de lancer Média virtuel lorsque la **Console virtuelle** est désactivée, vérifiez que 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 accéder au média virtuel lorsque la console virtuelle est désactivée :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Média virtuel**.
2. Cliquez sur **Connecter un média virtuel**.

En outre, vous pouvez également lancer le média virtuel en procédant comme suit :

1. Accédez à **Configuration** > **Console virtuelle**.
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, voir Mappage de lecteur virtuel.
5. **Statistiques du média virtuel** affiche la liste des lecteurs cibles, leur mappage, leur état (en lecture seule ou non), la durée de la connexion, les octets en lecture/écriture et la vitesse de transfert.

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 : Le média virtuel peut ne pas fonctionner correctement sur les systèmes qui exécutent le système d'exploitation Windows et configurés avec la sécurité renforcée d'Internet Explorer. Pour résoudre le problème, voir la documentation du système d'exploitation ou contacter l'administrateur système.

Ajout d'images Média Virtuel

Vous pouvez créer une image de média du dossier distant 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 recherchez le dossier ou le répertoire à utiliser comme source pour le fichier image. Le fichier image se trouve sur la station de gestion ou sur le lecteur C: du système géré.
3. Dans le champ **Nouveau 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 modifier 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 vous ajoutez un dossier en tant qu'image, un fichier **.img** est créé sur le bureau de la station de gestion à partir de laquelle cette fonctionnalité est utilisée. Si ce fichier **.img** est déplacé ou supprimé, l'entrée correspondante à ce dossier dans le menu **Média virtuel** ne fonctionne pas. Par conséquent, il est recommandé de ne pas déplacer ou supprimer le fichier **.img** pendant l'utilisation de l'**image**. Il est toutefois possible de supprimer le fichier **.img** une fois l'entrée correspondante désélectionnée puis supprimée à l'aide de la fonction **Supprimer l'image**.

Affichage des informations détaillées d'un périphérique virtuel

Pour afficher les détails de l'appareil virtuel, dans la visionneuse de la console virtuelle, cliquez sur **Outils** > **Statistiques**. Dans la fenêtre **Statistiques**, la section **Média virtuel** affiche les appareils virtuels mappés et l'activité de lecture/écriture de chaque appareil. Si le média virtuel est connecté, ces informations s'affichent. Si le média virtuel n'est pas connecté, le message « Le média virtuel n'est pas connecté » s'affiche.

Si le média virtuel est lancé sans l'aide de la console virtuelle, la section **Média virtuel** s'affiche sous forme de boîte de dialogue. Celle-ci fournit des informations sur les appareils 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 iDRAC ne prend pas fin, même après que vous vous déconnectez de la session d'interface Web iDRAC.

Mappage d'un lecteur virtuel

Pour mapper un lecteur virtuel :

REMARQUE : Lors de l'utilisation d'un média virtuel, vous devez disposer des privilèges d'administration pour pouvoir mapper un DVD ou une clé USB d'un système d'exploitation (connecté à la station de gestion). Pour mapper ces lecteurs, lancez IE en tant qu'administrateur ou ajoutez l'adresse IP du contrôleur iDRAC à la liste des sites de confiance.

1. Pour établir une session de média virtuel, depuis le menu **Média virtuel**, cliquez sur **Connecter un 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 un périphérique externe

   L'option **Mappage de DVD/CD** peut être utilisée pour les fichiers ISO et l'option **Mappage de disque amovible** peut être utilisée pour les images avec un média virtuel basé sur ehtml5. L'option **Mapper un périphérique externe** peut être utilisée pour le mappage des disques USB physiques.

   REMARQUE :
   - Vous ne pouvez pas mapper des supports physiques tels que les clés USB, les CD ou les DVD à l'aide de la console virtuelle HTML5.
   - Vous ne pouvez pas mapper les clés USB en tant que disques de support virtuel depuis Virtual Console (Console virtuelle) ou Virtual Media (Média virtuel) avec une session RDP.
   - Vous ne pouvez pas mapper des supports physiques avec le format NTFS dans les supports amovibles ehtml. Utilisez des périphériques FAT ou exFAT.

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 ou à partir d'une autre session d'interface Web.

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 et Disque amovible) et les types de fichiers 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 type de fichier approprié pour les CD/DVD est ISO, et IMG pour les disques amovibles.

   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 sur un autre emplacement, lorsque vous sélectionnez **Mapper le disque amovible**, l'image créée n'est pas disponible dans le menu déroulant. Cliquez sur **Parcourir** pour spécifier l'image.

REMARQUE : L'émulation de disquette n'est pas prise en charge dans le plug-in ehtml5.

4. Sélectionnez **Lecture seule** pour mapper les périphériques inscriptibles comme en lecture seule.

   Par défaut, cette option est activée pour les périphériques CD/DVD et vous ne pouvez pas la désactiver.

   REMARQUE : Les fichiers IMG et ISO sont mappés en tant que fichiers en lecture seule si vous mappez ces fichiers en utilisant la console virtuelle HTML5.

5. Cliquez sur **Mapper le périphérique** pour mapper le périphérique au serveur hôte.

   Une fois le périphérique/fichier adressé, 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 à un fichier image nommé `foo.iso`, l'élément du menu CD/DVD dans le menu Média virtuel se nomme **foo.iso mappé au CD/DVD**. Une coche en regard de cet élément de menu indique qu'il est mappé.

Affichage des lecteurs virtuels corrects pour le mappage

Sur une station de gestion Linux, la fenêtre **Client** du Média virtuel peut afficher les disques amovibles qui ne font pas partie de la station de gestion. Pour vérifier que les disques virtuels appropriés sont disponibles pour le mappage, vous devez activer le paramètre de port pour le disque dur SATA connecté. Pour ce faire, procédez comme suit :

1. Redémarrez le système d'exploitation sur la station de gestion. Lors de l'autotest de démarrage, appuyez sur <F2> pour accéder à **Configuration du système**.
2. Accédez à **Paramètres SATA**. Les informations du port s'affichent.
3. Activez les ports présents et connectés au disque dur.
4. Accédez à la fenêtre **Client** du Média virtuel. Elle affiche les lecteurs adéquats qui peuvent être mappés.

Effacement du cache Java

En cas d'erreurs inattendues lors de l'utilisation de l'USB, effacez le cache Java. Pour effacer le cache Java, procédez comme suit :

1. Dans le Panneau de configuration Java, sous l'onglet **Général**, cliquez sur **Paramètres** sous la section **Fichiers Internet temporaires**. La boîte de dialogue **Paramètres des fichiers temporaires** s'affiche.
2. Cliquez sur **Supprimer des fichiers** dans la boîte de dialogue Paramètres des fichiers temporaires.

   La boîte de dialogue **Supprimer des fichiers et applications** s'affiche.
3. Cliquez sur **OK** dans la boîte de dialogue **Supprimer des fichiers et applications**. Cela supprime toutes les applications et applets téléchargées du cache.
4. Cliquez sur **OK** dans la boîte de dialogue **Paramètres des fichiers temporaires**. Si vous souhaitez supprimer une application et une applet spécifiques du cache, cliquez respectivement sur les options « Afficher l'application » et « Afficher l'applet ».

Dissociation d'un lecteur virtuel

Pour dissocier le 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**.

   Le message qui apparaît vous demande de confirmer.
2. Cliquez sur **Oui**.

   La coche en regard de cet élément de menu n'apparaît pas ; ce qui indique qu'il n'est pas mappé au serveur hôte.

   REMARQUE : Après l'annulation du mappage d'un périphérique USB connecté à vKVM à partir d'un système client exécutant le système d'exploitation Macintosh, il est possible que le périphérique non mappé ne soit pas disponible sur le client. Redémarrez le système ou montez manuellement le périphérique sur le système client pour afficher le périphérique.

REMARQUE : Pour annuler le mappage d'un lecteur de DVD virtuel sous Linux, démontez le lecteur et éjectez-le.

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 d'iDRAC, accédez à **Présentation** > **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.

Partage de fichier à distance

Cette fonctionnalité est disponible uniquement sous licence iDRAC Enterprise ou Datacenter.

Les montages de partage de fichier à distance (RFS) peuvent modifier l'attribut Lecture-écriture et sont pris en charge à partir de RACADM/Redfish uniquement.

REMARQUE : Avant d'utiliser la fonctionnalité RFS, assurez-vous que vous disposez d'une bande passante réseau minimale de 1 Mo/s.

Partage de fichier à distance 1 (RFS1)

La fonctionnalité de partage de fichier à distance 1 (RFS1) utilise l'implémentation de média virtuel dans iDRAC.

Lorsqu'un fichier image est monté à l'aide de la fonctionnalité RFS1, les deux lecteurs de disques virtuels Média virtuel sont visibles au système d'exploitation hôte. Si un fichier **.img** est mappé, et que le lecteur virtuel de disquettes/disques durs est ensuite utilisé pour présenter le fichier image au système d'exploitation. Si un fichier **.iso** est mappé, et que le lecteur virtuel de CD/DVD est ensuite utilisé pour présenter le fichier image au système d'exploitation. Le lecteur virtuel non utilisé apparaît au système d'exploitation comme un lecteur vide. Le client Média virtuel peut mapper des images ou des disques durs aux deux lecteurs virtuels, mais le RFS ne peut utiliser qu'un lecteur à la fois. RFS et les fonctionnalités de média virtuel sont mutuellement exclusifs.

REMARQUE :

- RFS1 s'affiche en tant que lecteur optique virtuel ou lecteur de disquette lorsqu'il n'y a pas de session de média virtuel active, en fonction de l'image rattachée.
- RFS1 s'affiche en tant que fichier réseau virtuel 1 lorsqu'il existe une session de média virtuel active, car le lecteur optique virtuel et les lecteurs de disquette virtuels sont consommés avec le média virtuel.

Saisissez les informations requises et cliquez sur **Se connecter** pour vous connecter au RFS1. Pour vous déconnecter de RFS1, cliquez sur **Déconnecter**. Pour en savoir plus sur les informations de champ obligatoires, voir l'**Aide en ligne** dans l'interface utilisateur de l'iDRAC.

REMARQUE :

- Le délai d'expiration de l'iDRAC pour la connexion RFS est de 55 secondes. Si la connexion prend plus de 55 secondes, l'erreur de délai d'expiration s'affiche.
- L'authentification de base et l'authentification Digest pour les partages HTTP/HTTPS sont pris en charge.
- **Connecter** est désactivé si la fonctionnalité RFS n'est pas sous licence. L'option **Déconnecter** est toujours disponible, quel que soit l'état de la licence. Cliquez sur **Déconnecter** pour déconnecter une connexion RFS existante.

Scénarios

- 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 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 de Média virtuel.
- Si la session RFS1 est active et que vous tentez d'établir une connexion vMedia, la connexion vMedia est refusée.
- Si le client Média virtuel est actif et que vous tentez d'établir une connexion RFS, il est possible que le lecteur optique virtuel/la disquette virtuelle attribué au média virtuel et au fichier réseau virtuel 1 soit attribué à RFS.

Partage de fichier à distance 2 (RFS2)

Le partage de fichier à distance 2 (RFS2) est indépendant de RFS1 et du média virtuel. RFS2 possède sa propre copie des attributs indépendamment de RFS1. L'option d'image RFS2 a le même comportement que le RFS1 existant sur toutes les interfaces iDRAC. Les deux sont autorisés à se connecter/se déconnecter indépendamment. Le RFS2 est contrôlé à l'aide des attributs Activé/Désactivé et Mode de connexion RFS2.

Pour démarrer avec le fichier réseau virtuel RFS2 2, sélectionnez **Fichier réseau virtuel 2** dans les options de démarrage. Le démarrage du média virtuel n'a aucun impact sur RFS2 lorsqu'il est activé.

Saisissez les informations requises, puis cliquez sur **Se connecter** pour vous connecter à RFS2, puis sur **Se déconnecter** pour vous déconnecter de RFS2.

Lorsque vous téléchargez/supprimez un certificat HTTPS dans RFS1, le certificat est également téléchargé/supprimé dans RFS2, car le certificat est destiné à identifier l'iDRAC et il reste identique pour plusieurs RFS et toutes les connexions partagées.

L'état de la connexion RFS est disponible dans le journal iDRAC. Une fois connecté, un lecteur virtuel monté avec la fonction RFS n'est pas déconnecté, même si vous vous déconnectez du contrôleur iDRAC. La connexion RFS est fermée en cas de réinitialisation de l'iDRAC ou de perte de la connexion réseau.

Si vous mettez à jour le firmware de l'iDRAC 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 firmware, et l'iDRAC redémarre.

Si vous mettez à jour le firmware de l'iDRAC 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 firmware, et l'iDRAC redémarre.

REMARQUE :

- CIFS et NFS prennent en charge à la fois les adresses IPv4 et IPv6.
- Lors de la connexion à un partage de fichiers distant à l'aide d'IPv6 en fournissant un nom de domaine complètement qualifié, IPv4 doit être désactivé sur le serveur HTTPS.
- Lorsque le contrôleur iDRAC est configuré avec les deux protocoles IPv4 et IPv6, le serveur DNS peut contenir des enregistrements associant le nom d'hôte du contrôleur iDRAC aux deux adresses. Si l'option IPv4 est désactivée dans le contrôleur iDRAC, celui-ci peut ne pas être en mesure d'accéder au partage IPv6 externe. Cela est dû au fait que le serveur DNS peut encore contenir des enregistrements IPv4 et que la résolution de nom DNS peut retourner l'adresse IPV4. Dans un cas comme celui-ci, nous vous recommandons de supprimer les enregistrements DNS IPv4 du serveur DNS au moment de désactiver l'option IPv4 dans le contrôleur iDRAC.
- Si vous utilisez CIFS et faites partie d'un domaine Active Directory, entrez le nom de domaine et l'adresse IP dans le chemin d'accès du fichier image.
- Pour accéder à un fichier à partir d'un partage NFS, configurez les autorisations de partage suivantes. Ces autorisations sont requises, car les interfaces iDRAC sont exécutées en mode non root.
  - Linux : vérifiez que les autorisations de partage sont définies sur au minimum **Lecture** pour le compte **Autres**.
  - Windows : accédez à l'onglet **Sécurité** dans les propriétés de partage et ajoutez **Tout le monde** au champ **Noms d'utilisateur ou de groupes** avec le privilège **Lecture et exécution**.
- 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.
- Seuls les caractères anglais ASCII sont pris en charge dans les chemins de fichiers sur un partage réseau.
- La fonctionnalité d'éjection du lecteur du système d'exploitation n'est pas prise en charge lorsque le média virtuel est connecté à l'aide de la fonction RFS.
- RFS peut être déconnecté lorsque l'adresse IP de l'iDRAC n'est pas accessible pendant plus d'une minute. Essayez de le remonter une fois le réseau opérationnel.
- Lorsque vous indiquez les paramètres de partage réseau, il est conseillé d'éviter l'utilisation des caractères spéciaux dans le nom d'utilisateur et mot de passe ou de chiffrer en pourcentage les caractères spéciaux.
- Les caractères suivants sont pris en charge pour les champs **Nom d'utilisateur**, **Mot de passe** et **Chemin d'accès au fichier image** :

- A-Z
- a-z
- 0 à 9
- Caractères spéciaux : . _ - ? < > / \ :* | @
- Espace libre

- Pour HTTP, n'utilisez pas les caractères suivants : ! @ # % ^. Ces caractères sont pris en charge sur d'autres types de partage. Cependant, pour maintenir la compatibilité, utilisez les caractères recommandés.

Montage de dossier via RFS

L'iDRAC prend en charge le montage de dossiers directement via RFS. Cette fonctionnalité vous permet de joindre un dossier directement sans le convertir en fichier ISO/IMG.

REMARQUE :

- Cette fonctionnalité est disponible avec la licence iDRAC Enterprise ou Datacenter.
- Joindre des dossiers est possible uniquement via un partage NFS et CIFS. Les partages via HTTP/HTTPS ne sont pas pris en charge
- La taille du dossier NFS/CIFS à joindre est limitée à 1 Go et le nombre maximal de sous-dossiers est limité à 1 000.
- Il n'est pas possible de mapper un dossier vide.

Les scénarios suivants expliquent comment RFS1 et RFS2 sont répertoriés dans l'ordre de démarrage du BIOS :

Scénario 1 :

Si le média virtuel est déjà connecté à l'aide de la console virtuelle, l'ordre de démarrage du BIOS signale les périphériques en tant que **lecteur optique virtuel** ou **lecteur de disquette virtuel** en fonction du type d'image. Lorsque le périphérique RFS 1 est connecté, l'ordre de démarrage du BIOS le signale comme **Fichier réseau virtuel 1**. Pour le périphérique RFS 2, l'ordre de démarrage du BIOS le signale comme **Fichier réseau virtuel 2**.

Scénario 2 :

Lorsqu'aucun média virtuel n'est connecté et que vous rattachez un périphérique RFS 1, l'ordre de démarrage du BIOS le signale comme **lecteur optique virtuel** ou **lecteur de disquette virtuel** en fonction du type d'image. Lorsque vous rattachez un périphérique RFS 2, l'ordre de démarrage du BIOS le signale comme **Fichier réseau virtuel 2**.

Scénario n° 3

Lorsque le support virtuel n'est pas connecté et que RFS1 est joint :

- Lecteur optique virtuel pour l'image ISO
- Lecteur de disquette virtuel pour l'image IMG

La session du support virtuel sera bloquée, car la session RFS1 est active.

Lorsque le support virtuel est connecté et que RFS1 est rattaché, RFS1 est répertorié en tant que Fichier réseau virtuel 1 pour l'image ISO/IMG. Le but est de maintenir la compatibilité avec les vMedia et RFS existants, qui n'en autorisent qu'un seul à la fois. RFS2 est répertorié en tant que **Fichier réseau virtuel 2**, indépendamment du support virtuel et de RFS1.

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, les lecteurs de disquette virtuels, le fichier réseau virtuel 1 et le fichier réseau virtuel 2 sont répertoriés avec les périphériques de démarrage standard.
4. Assurez-vous que le lecteur virtuel est activé et répertorié en tant que premier périphérique doté d'un support amorçable. Si nécessaire, suivez les instructions qui s'affichent à l'écran pour modifier l'ordre de démarrage.

5. Cliquez sur **OK**, revenez à la page **Paramètres BIOS du système** et cliquez sur **Terminer**.
6. Cliquez sur **Oui** pour enregistrer les modifications et quitter.

   Le système géré redémarre.

   Le système géré tente de démarrer à partir d'un périphérique amorçable en fonction de l'ordre de démarrage. Si le périphérique virtuel est connecté et qu'un support amorçable est présent, le système démarre à partir du périphérique virtuel. Dans le cas contraire, le système oublie le périphérique, à l'instar d'un périphérique physique sans support amorçable.

Accès aux pilotes

Les serveurs Dell PowerEdge disposent de tous les pilotes du système d'exploitation pris en charge intégrés dans la mémoire flash du système. À l'aide de l'iDRAC, vous pouvez installer ou désinstaller les pilotes facilement pour déployer le système d'exploitation sur votre serveur.

Pour installer les pilotes :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Média virtuel**.
2. Cliquez sur **Monter des pilotes**.
3. Sélectionnez le système d'exploitation à partir de la fenêtre contextuelle et cliquez sur **Monter des pilotes**.

REMARQUE : La durée d'exposition est de 18 heures, par défaut.

Pour désinstaller les pilotes après l'installation :

1. Accédez à **Configuration** > **Média virtuel**.
2. Cliquez sur **Démonter les pilotes**.
3. Cliquez sur **OK** dans la fenêtre contextuelle.

REMARQUE : L'option **Monter des pilotes** peut ne pas s'afficher si le pack de pilotes n'est pas disponible sur le système. Assurez-vous de télécharger et installer la dernière version du pack de pilotes à partir de Page de support Dell.

26

Déploiement de systèmes d'exploitation

Vous pouvez utiliser n'importe quel utilitaire pour déployer des systèmes d'exploitation sur les systèmes gérés :

- Partage de fichier à distance
- Guide d'utilisation de la console

Sujets :

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'iDRAC sont activés pour l'utilisateur.
- Le partage réseau contient des pilotes et un fichier d'image amorçable du système d'exploitation dans un format standard, tel que **.img**, **.iso** ou **folder path**.

> **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, CIFS (Common Internet File Sharing), HTTP ou HTTPs.
2. Accédez à **Configuration** > **Paramètres système** > **Paramètres matériel** > **Premier périphérique d'amorçage**.
3. Définissez la séquence de démarrage dans la liste **Premier périphérique de démarrage** pour sélectionner un support virtuel tel qu'une disquette, un CD, un DVD, un ISO, un fichier réseau virtuel 1 et un fichier réseau virtuel 2.
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.

Gestion des partages de fichiers à distance

Avec la fonctionnalité de partage de fichier à distance (RFS), vous pouvez définir un fichier image ISO ou IMG situé sur un partage 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, CIFS, HTTP ou HTTPs. Cette fonction est disponible sous licence.

Le partage de fichiers à distance prend en charge les fichiers image au format **.IMG** et **.ISO**. Un fichier **.img** est redirigé en tant que disquette virtuelle et un fichier **.iso** est redirigé en tant que CD-ROM virtuel.

Vous devez posséder les privilèges Média Virtuel pour pouvoir effectuer un montage de RFS.

Cette fonctionnalité est disponible uniquement sous licence iDRAC Enterprise ou Datacenter.

Configuration du partage de fichier à distance à l'aide de l'interface web

Pour activer le partage de fichier à distance :

1. Dans l'interface Web de l'iDRAC, accédez à **Configuration** > **Média virtuel** > **Média connecté**.
   La page **Média connecté** s'affiche.
2. Sous **Médias connectés**, sélectionnez **Connecter** ou **Connecter automatiquement**.
3. Sous **Partage de fichier à distance**, indiquez le chemin d'accès au fichier d'image, le nom de domaine, le nom d'utilisateur et le mot de passe. Pour plus d'informations sur les champs, voir l'**Aide en ligne d'iDRAC**.

   Exemple de chemin d'accès à un fichier d'image :

   - CIFS — `//<IP to connect for CIFS file system>/<file path>/<image name>`
   - NFS — `< IP to connect for NFS file system>:/<file path>/<image name>`
   - HTTP — `http://<URL>/<file path>/<image name>`
   - HTTPs — `https://<URL>/<file path>/<image name>`

   REMARQUE : Pour éviter des erreurs d'E/S lorsque vous utilisez des partages CIFS hébergés sur des systèmes Windows 7, modifiez les clés de registre suivantes :

   - Définissez HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache sur `1`
   - Définissez HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size sur `3`

   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.

   REMARQUE : Pour plus d'informations sur les caractères recommandés pour les noms d'utilisateur et les mots de passe, reportez-vous à la section Caractères recommandés dans les noms d'utilisateur et les mots de passe.

   REMARQUE : Les caractères autorisés dans les noms d'utilisateur et les mots de passe pour les partages réseau sont déterminés par le type de partage réseau. L'iDRAC prend en charge les caractères valides pour les informations d'identification de partage réseau, telles que définies par le type de partage, à l'exception des caractères <, > et , (virgule).

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.

   REMARQUE : Si le chemin de l'image contient les références de l'utilisateur, utilisez le protocole HTTPS pour éviter que ces références ne s'affichent dans l'interface utilisateur graphique (GUI) et RACADM. Si vous saisissez les références dans l'URL, évitez d'utiliser le symbole « @ », car il s'agit d'un caractère de séparation.

   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 de CD est `/dev/sr0` et le périphérique de disquette est /dev/sdc. Pour utiliser le périphérique correct (pour SLES ou RHEL) lorsque vous connectez le périphérique virtuel, vous devez exécuter immédiatement la commande sur le système d'exploitation Linux :

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

Cela affiche le texte qui identifie le périphérique (par exemple sdc pour un périphérique SCSI). Cette procédure s'applique également à Média virtuel lorsque vous utilisez les distributions Linux au niveau d'exécution init 3. Par défaut, le média virtuel n'est pas monté automatiquement au niveau d'exécution init 3.

Configuration du partage de fichier à distance à l'aide de 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 l'image

`-d` : déconnecter l'image

`-u` <username> : nom d'utilisateur pour accéder au dossier partagé

`-p` <password> : mot de passe pour accéder au dossier partagé

`-l` <image_location> : emplacement de l'image sur le partage réseau ; utilisez des guillemets autour de l'emplacement. Voir des exemples de chemin d'accès au fichier image dans la section Configuration du partage de fichiers à distance à l'aide de l'interface Web

`-s` : affiche l'état actuel de l'image distante

Exemples d'utilisation

- RFS basé sur CIFS :

```
racadm remoteimage -c -u "user" -p "pass" -l //shrloc/foo.iso
```

- RFS basé sur NFS :

```
racadm remoteimage -c -u "user" -p "pass" -l <nfs ip>:/shrloc/foo.iso
```

- RFS basé sur HTTP/HTTPS :

```
racadm remoteimage -c -u "user" -p "pass" -l http://url/shrloc/foo.iso
```

```
racadm remoteimage -c -l https://url/shareloc/foo.iso
```

- Déconnectez-vous de l'image distante :

```
racadm remoteimage -d
```

- Afficher l'état actuel de l'image distante :

```
racadm remoteimage -s
```

REMARQUE : Cette commande prend en charge les formats IPV4 et IPV6. IPV6 s'applique aux partages distants de type CIFS et NFS.

REMARQUE : Les options -u et -p sont obligatoires si le type de partage est cifs.

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).

REMARQUE : Pour éviter des erreurs d'E/S lorsque vous utilisez des partages CIFS hébergés sur des systèmes Windows 7, modifiez les clés de registre suivantes :

- Définissez HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache sur `1`
- Définissez HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size sur `3`

Pour obtenir de l'aide sur l'affichage des propriétés d'un groupe, exécutez la commande – `racadm help get`.

Pour obtenir de l'aide sur la configuration des propriétés d'un groupe, exécutez la commande – `racadm help set`.

```
racadm>>help remoteimage2
```

REMARQUE : remoteimage2 -- rend une image ISO distante disponible au serveur Elle nécessite une licence de partage de fichiers distants.

Utilisation

```
racadm remoteimage2 -c -u <user> -p <pass> -l <image_location>
racadm remoteimage2 -d
racadm remoteimage2 -s
```

Les options sont les suivantes :

`-c` : connecter l'image

`-d` : déconnecter l'image

`-u` <username> : nom d'utilisateur pour accéder au dossier partagé

`-p` <password> : mot de passe pour accéder au dossier partagé

`-l` <image_location> : emplacement de l'image sur le partage réseau ; utilisez des guillemets autour de l'emplacement. Voir des exemples de chemin d'accès au fichier image dans la section Configuration du partage de fichiers à distance à l'aide de l'interface Web

`-s` : affiche l'état actuel de l'image distante

Exemples d'utilisation

- RFS basé sur CIFS :

  ```
  racadm remoteimage2 -c -u "user" -p "pass" -l //shrloc/foo.iso
  ```

- RFS basé sur NFS :

  ```
  racadm remoteimage2 -c -u "user" -p "pass" -l <nfs ip>:/shrloc/foo.iso
  ```

- RFS basé sur HTTP/HTTPS :

  ```
  racadm remoteimage2 -c -u "user" -p "pass" -l http://url/shrloc/foo.iso
  ```

  ```
  racadm remoteimage2 -c -l https://url/shareloc/foo.iso
  ```

- Déconnectez-vous de l'image distante :

  ```
  racadm remoteimage2 -d
  ```

- Afficher l'état actuel de l'image distante :

  ```
  racadm remoteimage2 -s
  ```

REMARQUE : Cette commande prend en charge les formats IPV4 et IPV6. IPV6 s'applique aux partages distants de type CIFS et NFS.

REMARQUE : Les options -u et -p sont obligatoires si le type de partage est cifs.

Pour obtenir de l'aide sur l'affichage des propriétés d'un groupe, exécutez la commande – `racadm help get`.

Pour obtenir de l'aide sur la configuration des propriétés d'un groupe, exécutez la commande – `racadm help set`.

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 réseau contient des pilotes et un fichier d'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 iDRAC.
   - 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.

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.

27

Dépannage d'un système géré à l'aide d'iDRAC

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 ;
- État de santé du système

Sujets :

Utilisation de la console de diagnostic

L'iDRAC fournit un ensemble standard d'outils de diagnostic réseau similaires aux outils inclus avec les systèmes Microsoft Windows ou Linux. Vous pouvez accéder aux outils de débogage réseau à l'aide de l'interface Web de l'iDRAC.

Pour accéder à la console de diagnostic :

1. Dans l'interface Web d'iDRAC, accédez à **Maintenance** > **Diagnostics**.
   La page **Commande de la console de diagnostic** s'affiche.
2. Dans la zone de texte **Commande**, entrez une commande et cliquez sur **Envoyer**. Pour plus d'informations sur les commandes, voir l'**Aide en ligne de l'iDRAC**.
   Les résultats s'affichent sur la même page.

Réinitialiser l'iDRAC et réinitialiser l'iDRAC aux paramètres par défaut

1. Dans l'interface Web d'iDRAC, accédez à **Maintenance** > **Diagnostics**.
   Vous avez le choix parmi les options suivantes :
   - Cliquez sur **Réinitialiser l'iDRAC** pour réinitialiser l'iDRAC. Une opération normale de redémarrage est réalisée sur l'iDRAC. Après le redémarrage, actualisez le navigateur pour vous reconnecter à iDRAC.
   - Cliquez sur **Réinitialiser l'iDRAC aux paramètres par défaut** pour réinitialiser l'iDRAC aux paramètres par défaut. Lorsque vous cliquez sur **Réinitialiser l'iDRAC aux paramètres par défaut**, la fenêtre **Réinitialiser l'iDRAC aux paramètres par défaut** s'affiche. Cette action réinitialise l'iDRAC aux paramètres d'usine par défaut. Choisissez l'une des options suivantes :
     a. Conserver les paramètres utilisateur et réseau.
     b. Supprimez tous les paramètres et réinitialisez les utilisateurs à la valeur d'usine (valeur root/usine).
     c. Ignorer tous les paramètres et réinitialiser le nom d'utilisateur et le mot de passe.

2. Un message d'avertissement s'affiche. Cliquez sur **OK** pour continuer.

Planification de diagnostics automatisés à distance

Vous pouvez appeler à distance des diagnostics automatisés hors ligne sur un serveur de façon ponctuelle et renvoyer les résultats. Si les diagnostics requièrent un redémarrage, vous pouvez les relancer immédiatement ou les planifier pour le cycle de maintenance ou le redémarrage suivant (comme les mises à jour). Si 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 NFS, CIFS, HTTP ou HTTPS avec la commande racadm `diagnostics export`.

Vous devez disposer de la licence iDRAC 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 :

- Start time (Heure de début) : exécuter le diagnostic à un jour et une date ultérieurs. Si vous choisissez TIME NOW, le diagnostic est exécuté au prochain redémarrage.
- End time (Heure de fin) : exécuter le diagnostic à un jour et une heure ultérieurs à l'heure de début. S'il n'est pas lancé avant l'heure de fin, il est marqué comme en échec avec expiration de l'heure de fin. Si vous choisissez 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)
- Forced Graceful shutdown (Arrêt normal forcé) : le système d'exploitation s'arrête 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 planifiée ou exécutée en même temps. Une tâche de diagnostic peut être exécutée avec succès, exécutée avec erreur ou ne pas aboutir. Les événements de diagnostic, notamment les résultats, sont enregistrés dans le journal de Lifecycle Controller. Vous pouvez récupérer les résultats de la dernière exécution du diagnostic en utilisant l'interface RACADM à distance.

Vous pouvez exporter les résultats des derniers diagnostics effectués qui ont été planifiés à distance sur un partage réseau tel que CIFS ou NFS. La taille maximale du fichier est de 5 Mo.

Vous pouvez annuler une tâche de diagnostic lorsque l'état de la tâche est Unscheduled (Non planifié) ou Scheduled (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 et exportation des résultats 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 du diagnostic, assurez-vous que le serveur est à l'état **Hors POST** et que LC est à l'état **Prêt**. Pour vérifier l'état de LC et du serveur, exécutez la commande suivante :

  ```
  racadm getremoteservicesstatus
  ```

- 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 / HTTP / HTTPs share> -u
  <username> -p <password>
  ```

Pour plus d'informations sur les options, voir le Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

Affichage des codes du Post

Les codes POST sont des indicateurs de progression du BIOS du système, indiquant différentes étapes de la séquence de démarrage à partir de la réinitialisation de l'alimentation et vous permettant de diagnostiquer les pannes liées au démarrage du système. La page **Codes POST** affiche le dernier code POST du système avant le démarrage du système d'exploitation.

Pour afficher les codes POST, accédez à **Maintenance** > **Dépannage** > **Code 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 d'événements d'un cycle de démarrage. Les vidéos de cycle de démarrage sont triées par ordre des plus récentes aux plus anciennes.
- **Vidéo du dernier blocage** : une vidéo du blocage enregistre la séquence d'événements précédant le blocage.

REMARQUE : La fonctionnalité de vidéo de blocage est activée par défaut. Vous pouvez l'activer ou la désactiver selon vos besoins.

Il s'agit d'une fonctionnalité sous licence.

L'iDRAC enregistre 50 images lors du démarrage. La lecture des écrans de démarrage s'effectue à une vitesse d'1 image par seconde. Si l'iDRAC est réinitialisé, la vidéo de capture de démarrage n'est pas disponible, car elle est stockée dans la RAM, puis 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.
- L'heure de capture vidéo affichée dans le lecteur vidéo de l'interface utilisateur graphique de l'iDRAC peut différer de l'heure de capture vidéo affichée dans d'autres lecteurs vidéo. Le lecteur vidéo de l'interface utilisateur graphique de l'iDRAC affiche l'heure dans le fuseau horaire de l'iDRAC alors que tous les autres lecteurs vidéo affichent l'heure dans les fuseaux horaires respectifs du système d'exploitation.

REMARQUE :

- La cause du retard de disponibilité du fichier de capture du démarrage est due au fait que la mémoire tampon de celui-ci n'est pas pleine après le démarrage de l'hôte.
- Les lecteurs vidéo par défaut/intégrés SLES/RHEL ne prennent pas en charge le décodeur vidéo MPEG-1. Vous devez installer un lecteur vidéo compatible avec un décodeur MPEG et lire les fichiers.
- Les vidéos au format MPEG-1 ne sont pas prises en charge par le lecteur natif du système d'exploitation MAC.

Pour afficher l'écran de **Capture du démarrage**, cliquez sur **Maintenance** > **Dépannage** > **Capture vidéo**.

L'écran **Capture vidéo** affiche les enregistrements vidéo. Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.

REMARQUE : Lorsque le contrôleur vidéo intégré est désactivé et que le serveur dispose d'un contrôleur vidéo complémentaire, on peut s'attendre à une certaine latence par rapport à la capture de démarrage. Par conséquent, les messages de fin du processus POST d'une vidéo sont enregistrés lors de la prochaine capture.

Configuration des paramètres de capture vidéo

Pour configurer les paramètres de capture vidéo :

1. Dans l'interface Web de l'iDRAC, accédez à **Maintenance** > **Dépannage** > **Capture vidéo**.
   La page **Capture vidéo** s'affiche.
2. Dans le menu déroulant **Paramètres de capture vidéo**, sélectionnez l'une des options suivantes :
   - **Désactiver** : la capture de démarrage est désactivée.

- **Capturer tant que le tampon n'est pas saturé** : la séquence de démarrage est capturée jusqu'à ce que la taille du tampon ait été atteinte.
- **Capturer jusqu'à la fin de l'auto-test de démarrage (POST)** : la séquence de démarrage est capturée jusqu'à la fin de l'auto-test de démarrage (POST).

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

Affichage des journaux

Vous pouvez afficher les journaux des événements système (SEL) et les journaux Lifecycle. Pour plus d'informations, voir les sections Affichage des journaux des événements système et Affichage des journaux 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 iDRAC. Il s'agit d'une fonctionnalité 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 iDRAC, accédez à **Présentation** > **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.

   REMARQUE : Une fois l'iDRAC réinitialisé ou lorsqu'un événement de cycle d'alimentation secteur se produit, les données de capture du blocage sont effacées.

   REMARQUE : La résolution de l'écran du dernier blocage est toujours 1024x768, quelle que soit la résolution du système d'exploitation de l'hôte.

Affichage de l'état du système

La section État du système indique l'état des composants suivants du système :

- Résumé
- Batteries
- Refroidissement
- CPU
- Panneau avant
- Intrusion
- Mémoire
- Périphériques réseau
- Bloc d'alimentation
- Tensions

Affichage de l'état LED du panneau avant du système

Pour visualiser l'état actuel du voyant LED correspondant à l'ID système, dans l'interface Web de l'iDRAC, accédez à **Système** > **Présentation** > **Panneau avant**. La section **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 (état indiqué par une icône d'intégrité bleue sur le voyant LED du panneau avant), **Masquer l'erreur** et **Afficher l'erreur** sont grisées. Vous pouvez masquer ou afficher les erreurs uniquement pour les serveurs rack et de type tour.

Pour afficher l'état du voyant LED d'ID du système via RACADM, utilisez la commande `getled`.

REMARQUE : Lors du retrait à chaud du disque M.2 du contrôleur BOSS N-1, l'état d'intégrité du tableau de bord de l'iDRAC devient orange, mais le voyant LED d'intégrité avant/arrière du serveur reste bleu.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

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
- Dommages physiques

En fonction du problème, utilisez les méthodes suivantes pour éliminer le problème :

- Remettez le module ou le composant en place et redémarrez le système.
- 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 d'installation et de maintenance* disponible sur la page Manuels PowerEdge pour obtenir des informations de dépannage spécifiques sur le périphérique matériel.

PRÉCAUTION : N'effectuez que les opérations de dépannage et les petites réparations autorisées par la documentation de votre produit, et suivez les instructions fournies en ligne ou par téléphone par l'équipe de maintenance et de support technique. Tout dommage provoqué par une réparation non autorisée par Dell est exclu de votre garantie. Consultez et respectez les consignes de sécurité fournies avec votre produit.

Affichage de l'intégrité du système

Vous pouvez afficher l'état des composants suivants sur l'iDRAC :

- Batteries
- CPU
- Refroidissement
- Intrusion
- Mémoire
- Blocs d'alimentation
- Média flash amovible
- Tensions
- Divers

Cliquez sur un nom de composant dans la section **Intégrité du serveur** pour afficher des informations sur le composant.

Redémarrage d'iDRAC

Vous pouvez redémarrer iDRAC 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 iDRAC ou l'interface RACADM.

Réinitialisation d'iDRAC à l'aide de l'interface RACADM

Pour redémarrer iDRAC, utilisez la commande **racreset**.

Pour rétablir les opérations par défaut, utilisez les commandes suivantes :

- Télécharger le fichier des paramètres par défaut personnalisés : `racadm -r <iDracIP> -u <username> -p <Password> set -f <filename> -t xml --customdefaults`
- Enregistrer les paramètres actuels comme paramètres par défaut : `racadm -r <iDracIP> -u <username> -p <Password> set --savecustomdefaults`
- Télécharger les paramètres par défaut personnalisés : `racadm -r <iDracIP> -u <username> -p <Password> get -f <filename> -t xml --customdefaults`
- Rétablir les paramètres par défaut personnalisés : `Racadm -r <iDracIP> -u <username> -p <Password> racresetcfg -custom`

Réinitialisation d'iDRAC à l'aide de l'interface Web iDRAC

Pour réinitialiser l'iDRAC, procédez de l'une des manières suivantes dans l'interface Web iDRAC :

- Télécharger le fichier des paramètres par défaut personnalisés :
  - Accédez à **Configuration** > **Profil de configuration du serveur** > **Paramètres personnalisés par défaut** > **Télécharger les paramètres personnalisés par défaut**
  - Téléchargez le fichier **CustomConfigured.xml** personnalisé à partir du chemin d'accès au partage local
  - Cliquez sur **Appliquer**. Une nouvelle tâche de téléchargement des paramètres par défaut personnalisés est créée.
- Réinitialiser aux paramètres personnalisés par défaut :
  - Lorsque la tâche de téléchargement des paramètres par défaut personnalisés est créée, accédez à **Maintenance** > **Diagnostics**, puis cliquez sur l'option **Réinitialiser l'iDRAC aux paramètres par défaut**.
  - Sélectionnez l'option **Supprimer tous les paramètres** et définissez-la sur **Configuration par défaut personnalisée**.
  - Cliquez sur **Continuer** pour lancer la configuration Réinitialiser aux paramètres personnalisés par défaut.

Effacement des données système et utilisateur

REMARQUE : L'effacement des données système et utilisateur n'est pas pris en charge depuis l'interface graphique de l'iDRAC.

Vous pouvez effacer des composants système et des données utilisateur pour les composants suivants :

- Restauration des valeurs par défaut du BIOS
- Diagnostics intégrés
- Pack de pilotes de système d'exploitation intégré
- Données du Lifecycle Controller
- Restauration des valeurs par défaut d'iDRAC
- Écrasement des disques durs qui ne prennent pas en charge l'effacement sécurisé instantané (ISE)
- Réinitialisation du cache du contrôleur
- Effacement des disques durs, disques SSD et NVMe qui prennent en charge l'ISE
- Effacez toutes les applications du système d'exploitation.

Avant d'effectuer l'effacement du système, assurez-vous que :

- Vous disposez du privilège de contrôle du serveur iDRAC.
- Le Lifecycle Controller est activé.

L'option Données du Lifecycle Controller efface tout le contenu, tel que le journal LC, la base de données de configuration, le firmware de restauration, les journaux livrés de l'usine et les informations de configuration du SPI FP (ou carte adaptatrice de gestion).

REMARQUE : Le journal de Lifecycle Controller contient les informations relatives à la demande d'effacement du système et toutes les informations générées lors du redémarrage d'iDRAC. Toutes les informations précédentes sont supprimées.

Vous pouvez supprimer un ou plusieurs composants du système à l'aide de la commande **SystemErase** :

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

Où :

- bios : restauration des valeurs par défaut du BIOS
- diag : diagnostics intégrés
- drvpack : pack de pilotes intégrés du système d'exploitation
- lcdata : effacement des données du Lifecycle Controller
- idrac : rétablissement des valeurs par défaut de l'iDRAC
- overwritepd : écrasement des disques durs qui ne prennent pas en charge l'effacement sécurisé instantané (ISE)
- percnvcache : réinitialisation du cache du contrôleur
- secureerasepd : effacement des disques durs, disques SSD et NVMe qui prennent en charge l'ISE
- allapps : efface toutes les applications du système d'exploitation

REMARQUE : L'effacement sécurisé n'efface pas le **Firmware de restauration iDRAC** de la partition lorsque la commande `racadm systemerase lcdata` est utilisée.

REMARQUE : Si SEKM est activé sur le serveur, désactivez-le à l'aide de la commande `racadm sekm disable` avant d'utiliser cette commande. Cela peut empêcher le verrouillage de tous les appareils de stockage sécurisés par l'iDRAC si les paramètres SEKM sont effacés de l'iDRAC en exécutant cette commande.

Pour plus d'informations, rendez-vous sur le site Guide de la CLI RACADM de l'Integrated Dell Remote Access Controller.

REMARQUE : Le lien vers le Dell Tech Center s'affiche dans l'interface utilisateur de l'iDRAC sur les systèmes de marque Dell.

REMARQUE : Après avoir exécuté l'effacement du système, il se peut que des disques virtuels s'affichent encore. Exécutez CSIOR après l'effacement du système et le redémarrage de l'iDRAC.

REMARQUE : Dans les dernières versions d'iDRAC, la commande `LCWipe` est obsolète. Pour effectuer l'opération d'effacement du système, exécutez la commande `systemerase`.

Restauration des paramètres par défaut définis en usine d'iDRAC

Vous pouvez restaurer les paramètres par défaut définis en usine d'iDRAC à l'aide de l'utilitaire de configuration d'iDRAC ou de l'interface Web iDRAC.

Restauration des paramètres par défaut définis en usine d'iDRAC à l'aide de l'interface Web iDRAC

Pour restaurer les paramètres par défaut définis en usine d'iDRAC à l'aide de l'interface Web iDRAC :

1. Accédez à **Maintenance** > **Diagnostics**.
   La page **Diagnostics de la console** s'affiche.
2. Cliquez sur **Réinitialiser iDRAC sur les paramètres par défaut**.
   L'état d'achèvement s'affiche en pourcentage. L'iDRAC redémarre et les paramètres par défaut sont restaurés. L'adresse IP de l'iDRAC est réinitialisée et n'est pas accessible. Vous pouvez configurer l'adresse 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 de Configuration d'iDRAC

Pour restaurer les paramètres par défaut définis en usine d'iDRAC à l'aide de 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.

28

Intégration de SupportAssist dans l'iDRAC

SupportAssist vous permet de créer des collections SupportAssist et d'utiliser d'autres fonctionnalités SupportAssist pour surveiller votre système et votre datacenter. L'iDRAC fournit des interfaces d'application pour collecter des informations sur la plate-forme qui permettent aux services de support de résoudre les problèmes de plate-forme et de système. L'iDRAC vous aide à générer une collection SupportAssist du serveur, puis à l'exporter vers un emplacement de la station de gestion (local) ou vers un emplacement réseau partagé tel que FTP, TFTP (Trivial File Transfer Protocol), HTTP, HTTPS, CIFS (Common Internet File System) ou NFS (Network File Share). La collecte est générée au format ZIP standard. Vous pouvez envoyer cette collecte au support technique en vue d'un dépannage ou d'une collecte d'inventaires.

Sujets :

SupportAssist

REMARQUE : IDRAC10 ne prend pas en charge l'enregistrement SupportAssist. Vous pouvez également utiliser OpenManage Enterprise ou Passerelle de connexion sécurisée.

Vous pouvez générer et enregistrer une collecte localement ou sur un réseau.

SupportAssist

Une fois SupportAssist configuré, vous pouvez vérifier le tableau de bord SupportAssist pour afficher le **journal de collecte**. L'enregistrement n'est pas requis pour afficher ou envoyer le journal de collecte.

Journal de collecte

Le **journal de collecte** affiche les détails de **Date et temps de collecte, Type de collecte** (manuelle), **Données collectées** (sélection personnalisée, toutes les données), **État de la collecte** (terminée avec des erreurs, terminée) et **ID de tâche**. Vous pouvez envoyer la dernière collecte conservée dans l'iDRAC à Dell.

REMARQUE : Une fois générées, les informations du journal de collecte peuvent être filtrées pour supprimer les informations d'identification personnelle (PII) en fonction de la sélection de l'utilisateur.

Génération de la collecte SupportAssist

Pour générer les journaux du système d'exploitation et des applications, l'iDRAC Service Module doit être installé et en cours d'exécution dans le système d'exploitation hôte.

REMARQUE : La collecte SupportAssist prend plus de 10 minutes lorsqu'elle est exécutée à partir du système d'exploitation/de l'iDRAC en même temps qu'OMSA 10.1.0.0.

Si vous devez travailler avec le support technique sur un problème concernant un serveur, mais que les règles de sécurité restreignent une 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 d'outils de Dell et sans avoir accès à Internet depuis le système d'exploitation du serveur ou l'iDRAC.

Vous pouvez générer un rapport d'intégrité du serveur, puis exporter le journal de collecte :

- Sur un emplacement de la station de gestion (localement).
- Sur un emplacement réseau partagé, tel que CIFS (Common Internet File System) ou NFS (Network File Share). Pour exporter vers un partage réseau tel que CIFS ou NFS, la connectivité réseau directe au port réseau iDRAC partagé ou dédié est requise.
- À Dell.

La collecte SupportAssist est générée au format ZIP standard. La collecte peut contenir les informations suivantes :

- Inventaire du matériel de tous les composants (notamment des informations de configuration des composants du système et du micrologiciel, les journaux d'événements du système et de la carte mère, les informations d'état de l'iDRAC et les journaux de Lifecycle Controller).
- Informations sur le système d'exploitation et les applications.
- Journaux du contrôleur de stockage.
- Journaux de débogage de l'iDRAC
- Elle contient également un visualiseur HTML5 qui est immédiatement accessible une fois la collecte terminée.
- La collecte fournit une vaste quantité d'informations détaillées du système et des journaux dans un format convivial qui peuvent être affichées sans télécharger la collecte sur le site de support technique.

Une fois les données générées, vous pouvez afficher celles qui contiennent plusieurs fichiers XML et fichiers journaux.

Chaque fois que les données sont collectées, un événement est enregistré dans le journal du Lifecycle Controller. L'événement inclut des informations telles que l'utilisateur ayant lancé le rapport, l'interface utilisée, la date et l'heure de l'exportation.

Sous Windows, si WMI est désactivé, la collecte d'OS Collector est arrêtée et un message d'erreur s'affiche.

Vérifiez que les niveaux de privilèges sont appropriés et qu'aucun paramètre de pare-feu ou de sécurité n'empêche l'obtention des données de registre ou des logiciels.

Avant de générer le rapport d'intégrité, assurez-vous que :

- Le Lifecycle Controller est activé.
- La fonction Collecter l'inventaire système au redémarrage (CSIOR) est activée.
- Vous avez des droits de connexion et de contrôle du serveur.

Génération manuelle de la collecte SupportAssist à l'aide de l'interface Web d'iDRAC

Pour générer manuellement la collecte SupportAssist :

1. Dans l'interface Web de l'iDRAC, accédez à **Maintenance** > **SupportAssist**.
2. Cliquez sur **Lancer une collecte**.
3. Sélectionnez les ensembles de données à inclure dans la collecte.
4. Vous pouvez filtrer la collecte par informations personnelles identifiables.
5. Sélectionnez la destination où enregistrer la collecte.
   a. L'option **Enregistrer localement** permet d'enregistrer la collecte générée sur le système local.
   b. L'option **Enregistrer sur le réseau** enregistre la collecte générée dans l'emplacement de partage CIFS ou NFS défini par l'utilisateur.

      REMARQUE : Si l'option **Save to Network (Enregistrer sur le réseau)** est sélectionné et qu'aucun emplacement par défaut est disponible, les détails du réseau seront enregistrés comme emplacement par défaut pour les prochaines collectes. Si l'emplacement par défaut existe déjà, la collecte utilise les détails spécifiés une seule fois.

   Si l'option **Enregistrer sur le réseau** est sélectionnée, les informations relatives au réseau fournies par l'utilisateur sont enregistrées comme valeurs par défaut pour les collectes ultérieures (si aucun emplacement de partage réseau antérieur n'a été enregistré).
6. Cliquez sur **Collect** (Collecter) pour générer la collecte.
7. Si vous êtes invité, acceptez le contrat **Contrat de licence de l'utilisateur final, CLUF** pour continuer.

   L'option OS and Application Data (Données système d'exploitation et applications) est grisée car elle n'est pas sélectionnable :
   - Si iSM n'est pas installé ou en cours d'exécution sur le système d'exploitation hôte, ou
   - Si OS Collector a été supprimé de l'iDRAC, ou
   - Si la connexion directe OS-BMC est désactivée dans l'iDRAC, ou
   - Si les données du système d'exploitation et des applications ne sont pas disponibles dans une collecte précédente de l'iDRAC

Journal de collecte

Le **journal de collecte** affiche les détails de **Date et temps de collecte, Type de collecte** (manuelle), **Données collectées** (sélection personnalisée, toutes les données), **État de la collecte** (terminée avec des erreurs, terminée) et **ID de tâche**. Vous pouvez envoyer la dernière collecte conservée dans l'iDRAC à Dell.

REMARQUE : Une fois générées, les informations du journal de collecte peuvent être filtrées pour supprimer les informations d'identification personnelle (PII) en fonction de la sélection de l'utilisateur.

29

Questions fréquentes

Cette section contient les questions fréquentes sur les éléments suivants :

- Journal d'événements système
- Sécurité réseau
- Active Directory
- Authentification unique
- Ouverture de session avec une carte à puce
- Console virtuelle
- Support virtuel
- Authentification SNMP
- Périphériques de stockage
- iDRAC Service Module
- RACADM
- Divers

Sujets :

Système d'exploitation

Installation du système d'exploitation à l'aide des versions initiales d'iDRAC10 (1.10.17.00, 1.20.05.00)

L'interface utilisateur Lifecycle Controller n'est pas prise en charge sur l'iDRAC10. Vous pouvez installer le système d'exploitation à l'aide de la licence iDRAC10 de base.

Pour installer le système d'exploitation, procédez comme suit :

1. Créez un disque virtuel sur un contrôleur RAID de Dell :
   a. Appuyez sur **F2** pendant le processus de démarrage du système et accédez à la **configuration du système**.
   b. Cliquez sur **Paramètres de l'appareil** et sélectionnez contrôleur RAID approprié.
   c. Cliquez sur **Menu principal** > **Gestion de la configuration**.
   d. Cliquez sur **Créer un disque virtuel**.
   e. Sélectionnez les options appropriées pour définir les paramètres du disque virtuel.

f. Cliquez sur **Sélectionner des disques physiques** et sélectionnez les disques appropriés.
g. Cliquez sur **Appliquer les modifications**, puis sur **OK**.
h. Cliquez sur **Créer un disque virtuel**.
i. Sélectionnez **Confirmer**, puis cliquez sur **Oui**. Le disque virtuel est créé.

2. Installez le système d'exploitation à partir du DVD :
   a. Insérez le DVD d'installation du système d'exploitation.
   b. Démarrez à partir du DVD pour lancer le processus d'installation du système d'exploitation.
3. Téléchargez les disques manquants et installez le système d'exploitation :
   a. Téléchargez les pilotes requis pour le système d'exploitation à partir du site de support Dell.
   b. Copiez les pilotes téléchargés sur une clé USB.
   c. Lors de l'installation du système d'exploitation, lorsque vous êtes invité à saisir des pilotes, insérez la clé USB et chargez les pilotes à partir de celle-ci.

Active Directory

Échec de la connexion à Active Directory. Comment résoudre ce problème ?

Pour diagnostiquer le problème, accédez à la page **Configuration et gestion d'Active Directory**, puis cliquez sur **Tester les paramètres**. Examinez les résultats du test et corrigez le problème. Modifiez la configuration et exécutez le test jusqu'à ce que l'utilisateur réussisse l'étape d'autorisation.

En général, vérifiez les éléments suivants :

- Lorsque vous vous connectez, assurez-vous d'utiliser le nom de domaine d'utilisateur correct et pas le nom NetBIOS. Si vous disposez d'un compte d'utilisateur iDRAC local, connectez-vous à l'iDRAC à l'aide des informations d'identification locales. Après vous être connecté, vérifiez les points suivants :
  - 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 de réseau de l'iDRAC** .
  - Le certificat CA racine Active Directory correct est téléversé vers iDRAC 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.
  - Si l'utilisateur et l'objet iDRAC se trouvent dans un domaine différent, ne sélectionnez pas l'option **Domaine d'utilisateur depuis la connexion**. Sélectionnez plutôt l'option **Spécifier un domaine** et saisissez le nom de domaine où réside l'objet iDRAC.
- Vérifiez les certificats SSL des contrôleurs de domaine pour vous assurer que l'heure iDRAC est comprise dans la période de validité du certificat.

La connexion à Active Directory échoue même si la validation de certificat est activée. Le message d'erreur suivant s'affiche dans les résultats du test. Quelle est la cause de cette situation et comment résoudre le problème ?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct
Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if
the iDRAC date is within the valid period of the certificates and if the Domain Controller
Address configured in iDRAC matches the subject of the Directory Server Certificate.
```

Si la validation de certificat est activée, lorsque l'iDRAC établit la connexion SSL avec le serveur d'annuaire, il utilise le certificat CA chargé pour vérifier le certificat du serveur d'annuaire. Les principales causes de l'échec de la validation de certification sont les suivantes :

- La date de l'iDRAC n'est pas comprise dans la période de validité du certificat de serveur ou du certificat CA. Vérifiez l'heure de l'iDRAC et la période de validité du certificat.
- Les adresses de contrôleur de domaine configurées dans l'iDRAC ne correspondent pas au champ Objet ou Autre nom de l'objet du certificat du serveur d'annuaire. Si vous utilisez une adresse IP, lisez la question suivante. Si vous utilisez le FQDN, assurez-vous d'utiliser le FQDN du contrôleur de domaine et non du 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 de l'objet de votre certificat de contrôleur de domaine. En règle générale, Active Directory utilise le nom de l'hôte et non l'adresse IP du contrôleur de domaine dans le champ Objet ou Autre nom de l'objet du certificat de contrôleur de domaine. Pour résoudre ce problème, procédez de l'une des façons suivantes :

- Définissez le nom de l'hôte (nom de domaine complet) du contrôleur de domaine comme **adresse(s) de contrôleur de domaine** dans l'iDRAC 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 iDRAC.
- 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 de l'hôte (nom de domaine complet qualifié) ou de l'adresse IP du (ou des) contrôleur(s) de domaine qui gère(nt) le domaine dans lequel l'objet iDRAC réside.

Quand faut-il définir une adresse (ou des adresses) de catalogue global ?

Si vous utilisez le schéma standard et que tous les utilisateurs et groupes de rôles proviennent de domaines différents, une ou plusieurs adresses du catalogue global sont requises. Dans ce cas, vous ne pouvez utiliser que 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 ?

L'iDRAC se connecte d'abord aux adresses de contrôleur de domaine configurées. Si l'utilisateur et le groupe de rôles se trouvent dans ce domaine, les privilèges sont enregistrés.

Si une ou plusieurs adresses de contrôleur globales sont configurées, l'iDRAC continue d'interroger le catalogue global. Si des privilèges supplémentaires sont extraits du catalogue global, ces privilèges sont cumulés.

iDRAC utilise-t-il toujours LDAP sur SSL ?

Oui La totalité du transport s'effectue via le port sécurisé 636 et/ou 3269. Au cours du test, l'iDRAC exécute LDAP CONNECT uniquement pour isoler le problème, mais il n'exécute pas LDAP BIND sur une connexion non sécurisée.

Pourquoi iDRAC active-t-il par défaut la validation de certificat ?

L'iDRAC applique une sécurité renforcée pour garantir l'identité du contrôleur de domaine auquel il se connecte. Sans validation de certificat, un pirate informatique risque d'usurper un contrôleur de domaine et de pirater la connexion SSL. Si vous choisissez de faire confiance à tous les contrôleurs de domaine de votre périmètre de sécurité sans validation de certificat, vous pouvez la désactiver via l'interface Web ou RACADM.

iDRAC prend-il en charge le nom NetBIOS ?

Pas dans cette version.

Pourquoi l'ouverture de session dans iDRAC par carte à puce ou connexion directe (SSO) Active Directory prend-elle jusqu'à quatre minutes ?

La connexion via l'authentification unique ou par carte à puce à Active Directory prend normalement moins de 10 secondes, mais elle peut prendre jusqu'à quatre minutes si vous avez spécifié le serveur DNS et le serveur DNS auxiliaire que vous voulez utiliser sur la page Réseau, et que le serveur DNS a échoué. Des délais d'expiration DNS sont attendus lorsqu'un serveur DNS est arrêté. L'iDRAC vous permet de vous connecter en utilisant l'autre serveur DNS.

Active Directory est configuré pour un domaine présent dans Windows Server 2008 Active Directory. Un 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 de ce groupe. Lorsque vous tentez de vous connecter à l'iDRAC à l'aide de l'utilisateur présent dans le domaine enfant, la connexion SSO à Active Directory échoue.

Ce problème peut être dû à un type de groupe incorrect. Il existe deux types de groupes sur 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.

Vérifiez systématiquement que le type de groupe est défini sur Sécurité. Vous ne pouvez pas utiliser les groupes de distribution pour accorder une autorisation à un objet ; vous pouvez les utiliser pour filtrer les paramètres de stratégie de groupe.

iDRAC Service Module

Les détails de l'iSM sont manquants/ne sont pas mis à jour correctement sur la page de l'interface utilisateur graphique de l'iDRAC de certains serveurs PowerEdge

Lorsqu'un utilisateur ajoute des sous-NIC dans regroupement, la configuration est non valide. Par conséquent, iSM ne peut pas communiquer avec iDRAC correctement.

Comment vérifier si l'iDRAC Service Module est installé sur le système d'exploitation hôte ?

Pour savoir si l'iDRAC Service Module est installé sur votre système :

- Sur les systèmes exécutant Windows : ouvrez le **Panneau de configuration** et vérifiez si l'iDRAC Service Module est répertorié dans la liste des programmes installés affichés.
- Sur les systèmes exécutant Linux : exécutez la commande `rpm –qi dcism`. Si iDRAC Service Module est installé, l'état indiqué est **Installé**.
- Sur les systèmes exécutant ESXi : exécutez la commande `esxcli software vib list|grep -i open` sur l'hôte. IDRAC Service module s'affiche.

REMARQUE : Pour vérifier que l'iDRAC Service Module est installé sur Red Hat Enterprise Linux 7, utilisez la commande `systemctl status dcismeng.service` au lieu de la commande `init.d`.

Comment vérifier le numéro de version de l'iDRAC Service Module installé sur le système ?

Pour vérifier la version de l'iDRAC Service Module dans le système, effectuez l'une des opérations suivantes :

- Cliquez sur **Démarrer** > **Panneau de configuration** > **Programmes et fonctionnalités**. La version d'iDRAC Service Module installée est indiquée dans l'onglet **Version**.
- Accédez à **Poste de travail** > **Désinstaller ou modifier un programme**.

Quel est le niveau de permission minimal requis pour installer l'iDRAC Service Module ?

Pour installer l'iDRAC Service Module, vous devez disposer de privilèges Administrateur.

Le message suivant s'affiche dans le journal du système d'exploitation, même si la fonction de connexion directe entre le système d'exploitation et l'iDRAC sur USBNIC est configurée correctement. Pourquoi ?

L'iDRAC Service Module ne parvient pas à communiquer avec l'iDRAC à l'aide du canal de connexion directe entre l'OS et l'iDRAC

L'iDRAC Service Module utilise la fonction Connexion directe entre le SE et iDRAC sur NIC USB pour établir la communication avec l'iDRAC. Parfois, la communication n'est pas établie bien que l'interface de la NIC USB soit configurée avec l'adresse IP correcte. Ce problème peut survenir lorsque la table de routage du système d'exploitation hôte possède plusieurs entrées sous le même masque cible et que la destination NIC USB n'est pas la première dans la liste de l'ordre de routage.

Tableau 54. Exemple d'un ordre de routage

Destination	Passerelle	Masque générique	Indicateurs	Indicateur	Réf.	Utiliser Iface
default	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

Dans l'exemple, **enp0s20u12u3** est l'interface NIC USB. Le masque cible link-local est répété et la NIC USB n'est pas la première dans l'ordre. Cela entraîne un problème de connectivité entre l'iDRAC Service Module et iDRAC sur la Connexion directe entre le système d'exploitation et iDRAC. Pour résoudre le problème de connexion, assurez-vous que l'adresse IPv4 USBNIC iDRAC (la valeur par défaut est 169.254.1.1) est accessible depuis le système d'exploitation hôte.

Si ce n'est pas le cas :

- Modifiez l'adresse USBNIC iDRAC sur un masque cible unique.
- Supprimez les entrées qui ne sont pas nécessaires dans la table de routage pour vous assurer que la NIC USB est choisie par acheminement lorsque l'hôte tente d'accéder à l'adresse IPv4 de la NIC USB de l'iDRAC.

Où se trouve le journal Lifecycle répliqué sur le système d'exploitation ?

Pour afficher les journaux Lifecycle Controller répliqués :

Tableau 55. Emplacement des journaux Lifecycle

Système d'exploitation	Location
Microsoft Windows	**Observateur d'événements** > **Journaux Windows** > **Système**. Tous les journaux Lifecycle Cycle de l'iDRAC Service Module sont répliqués sous le nom de source **iDRAC Service Module**.

Tableau 55. Emplacement des journaux Lifecycle (suite)

Système d'exploitation	Location
	REMARQUE : Dans iSM version 2.1 et ultérieure, les journaux Lifecycle sont répliqués sous le nom de la source du journal Lifecycle Controller. Dans iSM version 2.0 et antérieure, les journaux sont répliqués sous le nom de la source d'iDRAC Service Module. **REMARQUE :** L'emplacement du journal Lifecycle peut être configuré en utilisant le programme d'installation d'iDRAC Service Module. Vous pouvez configurer l'emplacement lors de l'installation d'iDRAC Service Module ou en modifiant le programme d'installation.
Red Hat Enterprise Linux, SUSE Linux, CentOS et Citrix XenServer	`/var/log/messages`
VMware ESXi	`/var/log/syslog.log`

Quels sont les fichiers exécutables ou progiciels dépendants de Linux disponibles pour l'installation sous Linux ?

Pour afficher la liste des progiciels dépendants de Linux, voir la section **Linux Dependencies** (Dépendances Linux) dans le *Guide de l'utilisateur de l'iDRAC Service Module* disponible sur la page des manuels iDRAC..

Sécurité réseau

Lors de l'accès à l'interface Web de l'iDRAC, un avertissement de sécurité s'affiche pour indiquer que le certificat SSL émis par l'autorité de certification (CA) n'est pas de confiance.

L'iDRAC inclut un certificat de serveur par défaut iDRAC pour protéger le réseau lors de l'accès via l'interface Web et RACADM à distance. Ce certificat n'est pas émis par une autorité de certification de confiance. Pour résoudre ce problème, téléchargez un certificat de serveur iDRAC émis par une autorité de certification de confiance (par exemple, Microsoft Certificate Authority, Thawte ou Verisign).

Pourquoi le serveur DNS n'enregistre-t-il pas iDRAC ?

Certains serveurs DNS enregistrent les noms iDRAC qui contiennent jusqu'à 31 caractères.

Lors de l'accès à l'interface Web de l'iDRAC, un avertissement de sécurité s'affiche pour indiquer que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte de l'iDRAC.

L'iDRAC inclut un certificat de serveur par défaut iDRAC pour protéger le réseau lors de l'accès via l'interface Web et RACADM à distance. Lorsque ce certificat est utilisé, le navigateur Web affiche un avertissement de sécurité, car le certificat par défaut émis vers l'iDRAC ne correspond pas au nom d'hôte de l'iDRAC (par exemple, l'adresse IP).

Pour résoudre ce problème, téléchargez un certificat de serveur iDRAC émis vers l'adresse IP ou le nom d'hôte de l'iDRAC. Lors de la génération de la CSR (utilisée pour l'émission du certificat), veillez à ce que le nom commun (CN) de la CSR corresponde à l'adresse IP de l'iDRAC (si le certificat est émis vers l'adresse IP) ou au nom DNS enregistré de l'iDRAC (si le certificat est émis vers le nom enregistré de l'iDRAC).

Pour que la CSR corresponde au nom iDRAC DNS enregistré :

1. Dans l'interface Web de l'iDRAC, accédez à **Aperçu** > **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 iDRAC.
3. Cliquez sur **Appliquer**.

Pourquoi je ne parviens pas à accéder à l'iDRAC depuis mon navigateur web ?

Ce problème peut se produire si le HSTS (HTTP Strict Transport Security) est activé. Le HSTS est un mécanisme de sécurité Web qui permet aux navigateurs Web d'interagir en utilisant uniquement le protocole sécurisé HTTPS, et non HTTP.

Activez le protocole HTTPS sur votre navigateur et connectez-vous à l'iDRAC pour résoudre le problème.

Pourquoi je ne parviens pas à effectuer des opérations impliquant un partage CIFS à distance ?

Les opérations d'importation/exportation ou n'importe quelles autres opérations de partage de fichiers à distance qui impliquent un partage CIFS échouent si seul le protocole SMBv1 est utilisé. Assurez-vous que le protocole SMBv2 est activé sur le serveur fournissant le partage SMB/CIFS. Référez-vous à la documentation du système d'exploitation sur la façon d'activer le protocole SMBv2.

RACADM

Après avoir réinitialisé l'iDRAC (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 signifie ?

```
ERROR: Unable to connect to RAC at specified IP address
```

Le message indique que vous devez attendre qu'iDRAC 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 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 iDRAC, si le mode réseau bascule 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 iDRAC à partir de SUSE Linux Enterprise Server (SLES) 11 SP1.

Assurez-vous que les versions officielles openssl et libopenssl sont installées. Exécutez la commande suivante pour installer les packages RPM :

```
rpm -ivh --force < filename >
```

où `filename` correspond au fichier du package 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 RACADM distante et les services web ne sont plus disponibles après la modification d'une propriété. Pourquoi ?

Lorsque vous réinitialisez le serveur web iDRAC, il peut s'écouler un certain temps avant que les services RACADM distants et l'interface web ne redeviennent disponibles.

Le serveur web iDRAC est réinitialisé lorsque :

- Les propriétés de configuration réseau ou de sécurité réseau sont modifiées à l'aide de l'interface utilisateur web iDRAC.
- La propriété iDRAC.Webserver.HttpsPort est modifiée, y compris lorsqu'un fichier `racadm set -f <config file>` la modifie.
- La commande `racresetcfg` est utilisée.
- iDRAC est réinitialisé.
- Un nouveau certificat de serveur SSL est téléchargé.

Pourquoi un message s'affiche lorsque j'essaie de supprimer une partition après l'avoir créée en utilisant l'interface locale RACADM ?

Cette erreur se produit, car l'opération de création de partition est en cours. Toutefois, la partition est supprimée au bout d'un certain temps et un message indiquant la suppression de la partition s'affiche. Si ce n'est pas le cas, patientez jusqu'à ce que l'opération de création de partition soit terminée, puis supprimez la partition.

Configuration d'un e-mail d'expéditeur personnalisé pour les alertes iDRAC

L'e-mail généré par une alerte ne provient pas d'un e-mail d'expéditeur personnalisé défini sur un service de messagerie basé sur le Cloud.

Vous devez enregistrer votre e-mail dans le Cloud via ce processus : support.google.com.

Ouverture de session avec une carte à puce

L'ouverture de session dans iDRAC peut prendre jusqu'à quatre minutes à l'aide d'une carte à puce Active Directory.

La connexion à la carte à puce Active Directory prend normalement moins de 10 secondes, mais elle peut prendre jusqu'à quatre minutes si vous avez spécifié le serveur DNS et le serveur DNS auxiliaire que vous voulez utiliser sur la page **Réseau**, et si le serveur DNS a échoué. Des délais d'expiration DNS sont attendus lorsqu'un serveur DNS est arrêté. L'iDRAC vous permet de vous connecter en utilisant l'autre serveur DNS.

Le code PIN de la carte à puce est incorrect.

Vérifiez si la carte à puce est verrouillée en raison d'un trop grand nombre de tentatives de connexion avec un code PIN incorrect. Si c'est le cas, contactez l'émetteur de la carte à puce dans l'organisation pour obtenir une nouvelle carte à puce.

Authentification SNMP

Pourquoi le message « Accès distant : échec de l'authentification SNMP »' s'affiche-t-il ?

Dans le cadre de la détection, IT Assistant tente de vérifier les noms de communauté get et set de l'appareil. IT Assistant dispose de l'option get community name = public et de l'option set community name = private. Par défaut, le nom de communauté de l'agent SNMP pour l'iDRAC est public. Lorsque IT Assistant envoie une demande set, l'agent iDRAC génère l'erreur d'authentification SNMP, car il accepte uniquement les demandes provenant de community = public.

Pour empêcher la génération d'erreurs d'authentification SNMP, vous devez saisir des noms de communauté acceptés par l'agent. Étant donné que l'iDRAC n'autorise qu'un seul nom de communauté, vous devez utiliser le même nom de communauté get et set pour la configuration de la détection d'IT Assistant.

Authentification unique

La connexion SSO échoue sur Windows Server 2008 R2 x64. Quels sont les paramètres requis pour résoudre ce problème ?

1. Exécutez **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** pour le contrôleur de domaine et la stratégie de domaine.
2. Configurez les ordinateurs pour qu'ils utilisent la suite de chiffrement DES-CBC-MD5.

   REMARQUE : Ces paramètres peuvent avoir une incidence sur la compatibilité avec les ordinateurs clients ou les services et applications de votre environnement. Le paramètre Configurer les types de chiffrement autorisés pour la stratégie Kerberos se trouve à l'emplacement suivant : **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, saisissez `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 iDRAC.

Vous pouvez désormais ouvrir une session iDRAC via la connexion directe (SSO).

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 chiffrement pour Windows 7 et Windows Server 2008 R2. Pour activer les types de chiffrement :

1. Ouvrez une session comme administrateur ou utilisateur doté du privilège d'administration.

2. Cliquez sur **Démarrer** et exécutez **gpedit.msc**. La fenêtre **Éditeur de stratégie de groupe locale** 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 iDRAC via la connexion directe (SSO).

Définissez les paramètres supplémentaires suivants pour le schéma étendu :

1. Dans la fenêtre de l'**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. Cliquez sur **Démarrer** et exécutez la commande cmd. La fenêtre d'invite de commande s'affiche.
5. Exécutez la commande `gpupdate /force`. Les stratégies de groupe sont mises à jour. Fermez la fenêtre d'invite de commande.
6. Cliquez sur **Démarrer** et exécutez la commande regedit. La fenêtre **Éditeur du 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**, saisissez **1** et cliquez sur **OK**.
12. Fermez la fenêtre **Éditeur de registre**. Vous pouvez désormais ouvrir une session iDRAC via la connexion directe (SSO).

Si vous avez activé l'authentification unique pour l'iDRAC et utilisez Internet Explorer pour ouvrir une session dans l'iDRAC, l'authentification unique échoue et le système vous demande de saisir votre nom d'utilisateur et votre mot de passe. Comment résoudre ce problème ?

Assurez-vous que l'adresse IP de l'iDRAC est répertoriée dans la zone **Outils** > **Options Internet** > **Sécurité** > **Sites de confiance**. Si elle n'est pas répertoriée, l'authentification unique échoue et vous êtes invité à saisir votre nom d'utilisateur et votre mot de passe. Cliquez sur **Annuler** et continuez.

Périphérique de stockage

OpenManage Storage Management affiche plus de périphériques de stockage que l'iDRAC, pourquoi ?

L'iDRAC affiche des informations uniquement pour les appareils pris en charge par CEM (Comprehensive Embedded Management).

Pour les JBOD/Insights externes derrière l'adaptateur HBA, le message EEMI relatif au retrait du connecteur SAS/du module d'E/S est généré avec l'ID de message EEMI ENC42. Toutefois, les messages EEMI ENC41 et ENC1 relatifs à la restauration du connecteur SAS/du module d'E/S ne sont pas générés.

Pour confirmer la restauration du module d'E/S dans l'interface Web de l'iDRAC :

1. Accédez à **Stockage** > **Présentation** > **Boîtiers**.
2. Sélectionnez un boîtier.
3. Sous **Propriétés avancées**, assurez-vous que la valeur du champ **Chemins redondants** est définie sur **Présent**.

Pourquoi le numéro de série imprimé sur le périphérique PCIe est-il différent de celui indiqué dans l'interface utilisateur de l'iDRAC ?

Les périphériques basés sur la classe PCIe de base peuvent être de différents types et formats. Dans de tels scénarios, les numéros de série du périphérique peuvent différer de ceux d'un périphérique PCIe de base, notamment les formes dérivées de périphériques PCIe telles que les disques NVMe, les cartes NIC, etc.

Journal des événements système

Lors de l'utilisation de l'interface Web iDRAC via Internet Explorer, pourquoi le journal SEL ne peut-il pas être enregistré avec l'option Enregistrer sous ?

Ce problème est dû à un paramètre du navigateur. Pour remédier à ce problème :

1. Dans Internet Explorer, allez dans **Outils** > **Options Internet** > **Sécurité** et sélectionnez la destination pour le téléchargement. Par exemple, si l'appareil iDRAC se trouve sur l'intranet local, sélectionnez **Intranet local**, puis 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 iDRAC est fiable, sous Divers, désélectionnez l'option Démarrage des applications et des fichiers non sûrs.

Console virtuelle

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 iDRAC 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 ?

Nb

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 iDRAC pour démarrer ou arrêter la vidéo sur le serveur local ?

N'importe quel utilisateur doté des privilèges de configuration iDRAC 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.

Pour afficher l'état de l'objet `iDRAC.VirtualConsole.AttachState`, utilisez la commande suivante :

```
racadm get idrac.virtualconsole.attachstate
```

Ou bien utilisez la commande suivante depuis une session SSH ou distante :

```
racadm -r (iDrac IP) -u (username) -p (password) get iDRAC.VirtualConsole.AttachState
```

L'état est également visible dans l'affichage OSCAR de la console virtuelle. Lorsque la console locale est activée, un état de couleur verte apparaît en regard du nom du serveur. Lorsqu'elle est désactivée, un point jaune indique que l'iDRAC 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 De l'écran 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 sous Linux requiert 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 iDRAC est sélectionnée dans le client Console virtuelle iDRAC. 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 à distance un système d'exploitation Microsoft pris en charge sur un système sur lequel la console virtuelle est 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 à distance, refaire l'installation, puis arrêter la console virtuelle dans le BIOS.

Ce message est généré par Microsoft pour indiquer à l'utilisateur 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 y accédez via l'iDRAC, 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. 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 Mbit/s pour obtenir de bonnes performances. Une connexion de 1 Mbit/s minimum est nécessaire pour obtenir des performances minimales.

Quelle est la configuration matérielle 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 iDRAC ne reçoit pas la vidéo du bureau 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 bureau 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 de la plage permettant à l'iDRAC de capturer la vidéo. Si des paramètres, tels que la résolution d'affichage et le taux d'actualisation, ont une valeur trop élevée, cela génère un état hors plage. Normalement, les limitations physiques, telles que la taille de mémoire vidéo et la bande passante définissent la plage de valeurs maximales des paramètres.

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 fonctionnalité 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. De par sa conception, la souris PS/2 utilise la position relative du pointeur, ce qui entraîne un décalage dans la synchronisation. L'iDRAC dispose d'un pilote de souris USB qui permet une position absolue et un suivi plus précis du pointeur de la souris. Même si iDRAC 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 ce problème, définissez le mode souris sur USC/Diags dans l'écran 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 se produit si le **Mode Souris** est défini sur **USC/Diags**. Appuyez sur la touche d'accès rapide **Alt + M** pour utiliser la souris sur le système local. Appuyez à nouveau sur **Alt + M** pour utiliser la souris dans la console virtuelle.

Pourquoi la session de l'interface utilisateur graphique a expiré après avoir lancé une console virtuelle depuis l'interface de l'iDRAC lancée à partir du CMC ?

Lorsque vous démarrez la console virtuelle dans l'iDRAC 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 iDRAC depuis une station de gestion, une expiration de session se produit pour l'interface graphique iDRAC si l'interface graphique est démarrée avant la fermeture de la fenêtre contextuelle. Si vous démarrez l'interface graphique d'iDRAC depuis l'interface Web CMC après la fermeture de la fenêtre de lancement de la console virtuelle, le problème ne survient pas.

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 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 iDRAC en utilisant Internet Explorer :

1. Activez la fonction magic key (touche 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 fonctionnalité 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 tandis 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 Spanning Tree Protocol (STP) est activé sur le commutateur réseau connecté. 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.

Support virtuel

Pourquoi la connexion du client Média virtuel s'interrompt-elle parfois ?

Si le délai d'attente du réseau expire, le firmware d'iDRAC interrompt la connexion en déconnectant la liaison entre le serveur et le lecteur virtuel.

Si vous changez le CD sur le système client, la fonction de démarrage automatique peut être activée pour le nouveau CD. Si la lecture du CD prend trop de temps sur le système client, cela peut entraîner l'expiration du délai du firmware et la perte de la connexion. En cas de perte de la connexion, reconnectez-vous dans l'interface graphique et continuez l'opération précédente.

Si les paramètres de configuration de Virtual Media sont modifiés dans l'interface Web iDRAC ou via des commandes RACADM locales, tout support 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 Virtual Media prend-elle autant de temps ?

Lors de l'installation du système d'exploitation Windows en utilisant le DVD **Dell Systems Management Tools and Documentation**, si la connexion réseau est lente, l'accès à l'interface Web d'iDRAC durant l'installation peut nécessiter un certain temps du fait de la latence de 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 à la configuration du BIOS et au menu de démarrage. Recherchez le CD virtuel, la disquette virtuelle et changez la séquence d'amorçage selon les besoins. Appuyez sur la barre d'espacement dans la séquence de démarrage de la configuration CMOS afin que l'unité virtuelle devienne amorçable. Par exemple, pour effectuer le démarrage depuis un lecteur de CD, placez-le dans la première position de la séquence d'amorçage.

Quels sont les types de supports qui peuvent être définis comme périphériques amorçables ?

iDRAC 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 ?

Vous pouvez également effectuer le démarrage à partir d'un disque de démarrage Windows 98 et copier les fichiers système du disque de démarrage sur la clé USB. Par exemple, à l'invite du DOS, entrez la commande suivante :

```
sys a: x: /s
```

, où x: est la clé USB qui doit être définie comme périphérique amorçable.

Virtual Media est connecté à la disquette distante. Mais il ne détecte pas un lecteur de disquette ou CD virtuel sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux. Comment résoudre ce problème ?

Certaines versions de Linux effectuent le montage automatique du lecteur de disquette ou de CD virtuel en utilisant une autre méthode. Pour monter le lecteur de disquette virtuel, recherchez le nœud attribué par Linux au lecteur de disquette virtuel. Pour monter le lecteur de disquette virtuel :

1. Ouvrez une invite de commande Linux et exécutez la commande suivante :

   ```
   grep "Virtual Floppy" /var/log/messages
   ```
2. Recherchez la dernière entrée de ce message et notez l'heure.
3. 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 du périphérique identifié à l'étape 4 et `/mnt/floppy` est le point de montage.

Pour monter le lecteur de CD virtuel, recherchez le nœud attribué par Linux au lecteur de CD virtuel. Pour monter le lecteur de CD virtuel :

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 d'appareil 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 du périphérique identifié à l'étape 4 et `/mnt/floppy` est le point de montage.

Pourquoi les lecteurs virtuels connectés au serveur sont-ils supprimés après une mise à jour de firmware à distance à l'aide de l'interface Web iDRAC ?

Les mises à jour de firmware entraînent la réinitialisation de l'iDRAC, la désactivation de la connexion distante et le démontage des lecteurs virtuels. Les lecteurs réapparaissent à la fin de la réinitialisation de l'iDRAC.

Pourquoi tous les périphériques USB sont-ils déconnectés après la connexion d'un périphérique USB ?

Les unités Virtual Media sont connectées en tant qu'unités USB composites au BUS USB hôte et elles utilisent le même port USB. Lorsque vous connectez un support virtuel au bus USB hôte ou le déconnectez, toutes les unités Virtual Media sont provisoirement déconnectées du bus USB hôte puis reconnectées. Si le système d'exploitation hôte utilise une unité Virtual Media, ne connectez ni ne déconnectez aucune unité Virtual Media. Il est recommandé de connecter d'abord toutes les unités USB requises 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 de Virtual Media ?

Lancez Virtual Media avec la console virtuelle désactivée ou procédez de l'une des manières suivantes :

- Amenez le cureur des performances sur la vitesse maximale.
- Désactivez le chiffrement pour Virtual Media et la console virtuelle.

  REMARQUE : Dans ce cas, le transfert de données entre le serveur géré et iDRAC pour Virtual Media et la console virtuelle n'est pas sécurisé.

- Si vous utilisez un système d'exploitation de type serveur Windows, arrêtez le service Windows appelé Windows Event Collector (Collecteur d'événements de Windows). Pour ce faire, allez dans **Démarrer** > **Outils d'administration** > **Services**. Cliquez avec le bouton droit 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 Virtual Media ?

L'accès simultané à plusieurs lecteurs de disquette virtuels n'est pas autorisé. Fermez l'application utilisée pour afficher le contenu des lecteurs avant d'effectuer la virtualisation du 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 Virtual Media, même si Virtual Media n'est pas en cours d'utilisation ?

Ce message d'erreur s'affiche si la fonction de partage de fichiers à distance (RFS) est également utilisée. Vous pouvez utiliser la fonction RFS ou Virtual Media, mais pas les deux en même temps.

Divers

Pour les processeurs HBM (mémoire à bande passante élevée) en mode HBM, MemoryRollupStatus s'affiche comme Inconnu.

Pour le mode HBM uniquement, les données liées à la mémoire signalées dans l'inventaire du matériel, les capteurs, la télémétrie, etc., ne sont pas disponibles. Vous ne devez pas considérer qu'il s'agit d'une configuration défectueuse. Pour ces interfaces qui signalent tous les capteurs de logement DIMM individuels, ils sont déclarés avec l'état Inconnu. De même, le capteur de température DIMM max. peut également continuer à être signalé avec un état inconnu.

Lorsque vous tentez de connecter l'iDRAC à un autre réseau, l'iDRAC n'obtient pas d'adresse IP différente du nouveau sous-réseau.

Assurez-vous que le câble réseau est déconnecté de l'iDRAC pendant au moins 5 secondes.

Après la réinitialisation de l'iDRAC, l'interface utilisateur de l'iDRAC peut ne pas afficher toutes les valeurs.

REMARQUE : Si vous réinitialisez l'iDRAC pour quelque raison que ce soit, assurez-vous d'attendre au moins deux minutes après la réinitialisation d'iDRAC pour accéder aux paramètres d'iDRAC ou les modifier.

Si un système d'exploitation est installé, il est possible que le nom d'hôte ne s'affiche pas ou ne soit pas modifié automatiquement.

Deux cas sont possibles :

- Cas 1 : l'iDRAC n'affiche pas le dernier nom d'hôte après l'installation d'un système d'exploitation. Vous devez installer OMSA ou iSM avec l'iDRAC pour obtenir le nom d'hôte mise à jour.
- Cas 2 : l'iDRAC affichait un nom d'hôte propre à un système d'exploitation, puis un autre système d'exploitation a été installé mais l'ancien nom d'hôte continue à s'afficher et n'est pas remplacé par le nouveau. Le nom d'hôte étant une information provenant du

système d'exploitation, l'iDRAC ne fait qu'enregistrer cette information. Si un nouveau système d'exploitation est installé, l'iDRAC ne réinitialise pas la valeur du nom d'hôte. Cependant, les nouvelles versions des systèmes d'exploitation peuvent mettre à jour le nom d'hôte dans l'iDRAC lors du premier démarrage du système d'exploitation.

La connexion réseau iDRAC ne fonctionne pas.

Pour les serveurs au format rack et les serveurs tours:

- En mode partagé, vérifiez que le câble LAN est bien connecté au port NIC où figure le symbole de clé à molette.
- En mode dédié, vérifiez que le câble LAN est bien connecté au port LAN iDRAC.
- Vérifiez que les paramètres NIC, les paramètres IPv4 ou IPv6 et que Statique ou DHCP sont bien activés pour votre réseau.

L'iDRAC n'est pas accessible dans le LOM partagé

Il est possible que l'iDRAC soit inaccessible si des erreurs irrécupérables se sont produites dans le système d'exploitation hôte, notamment une erreur BSOD dans Windows. Pour accéder à l'iDRAC, redémarrez l'hôte pour rétablir la connexion.

LOM partagé non fonctionnel après l'activation du Link Aggregation Control Protocol (LACP).

Vous devez charger le pilote du système d'exploitation hôte de la carte réseau avant d'activer le protocole LACP. Cependant, si une configuration LACP passive est en cours d'utilisation, le LOM partagé peut fonctionner avant le chargement du pilote du système d'exploitation hôte. Consulter la configuration LACP dans la documentation du commutateur.

REMARQUE : L'IP du LOM partagé du contrôleur iDRAC n'est pas accessible à l'état préalable au démarrage lorsque le commutateur est configuré avec LACP.

Comment extraire le nom d'utilisateur et le mot de passe d'un administrateur iDRAC ?

Vous devez restaurer les paramètres par défaut d'iDRAC. Pour plus d'informations, voir Restauration des paramètres par défaut définis en usine d'iDRAC.

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 de montage vidéo n'est pas installée ou elle n'est pas connectée correctement.

Consultez également les messages d'erreur dans le journal iDRAC en utilisant l'interface Web de l'iDRAC .

Impossible de se connecter à l'interface Web de l'iDRAC à l'aide du navigateur Firefox sous Linux ou Ubuntu. Impossible de saisir le mot de passe.

Pour résoudre ce problème, réinstallez ou mettez à niveau le navigateur Firefox.

Impossible d'accéder à l'iDRAC via une carte réseau USB dans SLES et Ubuntu

REMARQUE : Dans SLES, définissez l'interface de l'iDRAC sur DHCP.

Dans Ubuntu, utilisez l'utilitaire Netplan pour configurer l'interface de l'iDRAC en mode DHCP. Pour configurer le mode DHCP :

1. Utilisez `/etc/netplan/01-netcfg.yaml`.
2. Indiquez Oui pour iDRAC via DHCP.
3. Appliquez la configuration.

Figure 5. Configuration de l'interface de l'iDRAC en mode DHCP dans Ubuntu

Le modèle, le fabricant et d'autres propriétés ne sont pas répertoriés pour les adaptateurs réseau intégrés dans Redfish

Les détails du FRU pour les périphériques intégrés ne seront pas affichés. Il n'existe aucun objet FRU pour les périphériques qui sont intégrés à la carte mère. Par conséquent, la propriété dépendante ne sera pas disponible.

Paramètres de serveur proxy

Comment configurer les paramètres du serveur proxy dans la CLI RACADM et l'API Redfish ?

Dans RACADM, les attributs LC suivants doivent être définis pour configurer le serveur proxy :

- LifeCycleController.LCAttributes.UserProxyPassword
- LifeCycleController.LCAttributes.UserProxyPort
- LifeCycleController.LCAttributes.UserProxyServer
- LifeCycleController.LCAttributes.UserProxyType
- LifeCycleController.LCAttributes.UserProxyUserName

Pour plus d'informations sur l'exécution de ces commandes, voir le **guide de la CLI de l'Integrated Dell Remote Access Controller**.

Lorsque vous utilisez HTTP avec un proxy, la connexion entre l'iDRAC et le proxy n'est pas aussi sécurisée que la connexion entre l'iDRAC et le serveur HTTPS. `UserProxyServer` est un attribut important. S'il n'est pas défini, les autres attributs ne peuvent pas être utilisés. L'avantage de l'utilisation de RACADM et de l'API Redfish est qu'il n'est pas nécessaire de fournir le mot de passe chaque fois que vous utilisez le serveur proxy.

Dans l'API Redfish, exécutez une opération de correctif à l'aide de l'URI `/redfish/v1/Managers/<Manager-ID>/Oem/Dell/DellAttributes/<Dell-attributes-ID>` pour configurer le serveur proxy.

Comment configurer les paramètres du serveur proxy dans l'interface utilisateur de l'iDRAC ?

Dans l'interface utilisateur de l'iDRAC, vous pouvez mettre à jour les paramètres proxy sur toutes les pages où le serveur proxy est requis. Même si vous avez configuré les paramètres proxy à l'aide de RACADM et de l'API Redfish, vous pouvez toujours mettre à jour les paramètres proxy dans l'interface utilisateur de l'iDRAC. Pour configurer les paramètres proxy dans la page **Mise à jour du système** :

1. Accédez à **Maintenance** > **Mise à jour du système** > **Mise à jour manuelle**.
2. Sous **Mise à jour manuelle**, sélectionnez **HTTPS** dans le champ **Type d'emplacement**.
3. Sélectionnez **Activé** sous **Activer le serveur proxy**.
4. Renseignez les champs **Serveur**, **Port**, **Nom d'utilisateur** et **Mot de passe**.
5. Sélectionnez le **Type** et cliquez sur **Enregistrer les paramètres proxy comme paramètres par défaut**.

REMARQUE : Vous pouvez configurer les paramètres proxy dans l'une des pages suivantes : **Exporter le journal Lifecycle**, **Mise à jour automatique**, **Paramètres de collecte SupportAssist**, **Importation du profil de configuration du serveur** et **Exportation du profil de configuration du serveur**.

REMARQUE : Par défaut, l'option **Activer les paramètres proxy** est désactivée dans l'interface utilisateur de l'iDRAC. Elle sera désactivée après chaque utilisation. Pour en savoir plus, voir l'**aide en ligne du contrôleur iDRAC (Integrated Dell Remote Access Controller)**.

Définition définitive du mot de passe par défaut pour calvin

Si votre système est livré avec un mot de passe iDRAC par défaut unique mais que vous voulez définir **calvin** en tant que mot de passe par défaut, vous devez utiliser les cavaliers disponibles sur la carte système.

PRÉCAUTION : La modification définitive des paramètres des cavaliers remplace le mot de passe par défaut par calvin. Vous ne pouvez pas rétablir le mot de passe unique, même si vous réinitialisez l'iDRAC aux paramètres d'usine.

Pour plus d'informations sur l'emplacement du cavalier et sur la procédure, voir la documentation de votre serveur à l'adresse Page de support Dell.

30

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.

Sujets :

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 datacenter 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 de l'iDRAC.

Avant de dépanner le système inaccessible, vérifiez si les conditions suivantes existent :

- Écran du dernier blocage activé
- Les alertes sont activées dans iDRAC

Pour identifier la cause, vérifiez les éléments suivants dans l'interface Web iDRAC et rétablissez la connexion au système :

- État du voyant du serveur : orange clignotant ou orange fixe.
- L'image du système d'exploitation s'affiche dans la console virtuelle. Si vous voyez l'image, réinitialisez le système (démarrage à chaud) et reconnectez-vous. Si vous parvenez à vous connecter, le problème est résolu.
- Écran du dernier blocage
- Vidéo de capture de démarrage.
- Vidéo de capture de blocage.
- État d'intégrité du serveur : icônes **×** 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 l'iDRAC Service Module

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 de l'iDRAC, accédez à **Présentation** > **Récapitulatif** pour afficher les informations système et accéder aux différents liens de cette page en vue d'évaluer l'intégrité du système.

- Si l'iDRAC Service Module est installé, les informations d'hôte du système d'exploitation s'affichent.

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 des événements système et du journal Lifecycle

Pour afficher et exporter le journal Lifecycle et le journal des événements système (SEL) :

1. Dans l'interface Web de l'iDRAC, accédez à **Maintenance** > **Journaux des événements système** pour afficher le journal SEL et à **Journal Lifecycle** pour afficher le journal Lifecycle.

   REMARQUE : Le journal SEL est également enregistré dans le journal Lifecycle. Utilisation des options de filtrage pour afficher le journal SEL.

2. Exportez le journal SEL ou le journal Lifecycle au format XML vers un emplacement externe (station de gestion, clé USB, partage réseau, etc.). Vous pouvez également activer la consignation système à distance, de sorte que tous les journaux écrits dans le journal Lifecycle soient également écrits simultanément sur le ou les serveurs distants configurés.
3. Si vous utilisez l'iDRAC Service Module, exportez le journal Lifecycle vers le journal du système d'exploitation.

Interfaces de mise à niveau du micrologiciel iDRAC

Utilisez les interfaces suivantes pour mettre à jour le micrologiciel iDRAC :

- l'interface web d'iDRAC
- API Redfish
- CLI RACADM
- Progiciel de mise à jour Dell (DUP - Dell Update Package)
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Exécution d'un arrêt normal

Le logiciel lance un arrêt normal en mettant le serveur hors tension, ce qui permet au système d'exploitation d'arrêter les processus en toute sécurité. Il met également hors tension les logements PCIe. Par conséquent, les adapatateurs dans les logements PCIe ne répondent pas aux commandes de contrôle NC-SI.

Si les commandes ne répondent pas, le module NIC-CEM traite les adaptateurs comme étant non réactifs et consigne les journaux HWC8607 Lifecycle Controller (LCLOG) pour indiquer que la communication avec les adaptateurs est perdue.

Pour exécuter un arrêt normal, dans l'interface Web de l'iDRAC, accédez aux emplacements suivants :

- Dans le **Tableau de bord**, sélectionnez **Arrêt normal**, puis cliquez sur **Appliquer**.

REMARQUE : Une fois la demande envoyée à l'hôte, il appartient à l'hôte d'honorer cette demande et de l'exécuter. La réussite de l'arrêt normal dépend de l'état de l'hôte.

Pour plus d'informations, voir l'**Aide en ligne de l'iDRAC**.

Création d'un compte utilisateur Administrateur

Vous pouvez modifier le compte d'utilisateur administrateur local par défaut ou en créer un nouveau. Pour modifier le compte d'utilisateur administrateur local, voir Modification des paramètres du compte d'administrateur local.

Pour créer un compte d'administrateur, voir les sections suivantes :

- Configuration des utilisateurs locaux
- Configuration des utilisateurs d'Active Directory
- Configuration d'utilisateurs LDAP générique

Lancement de la console distante des serveurs et montage d'un lecteur USB

Pour lancer la console distante et monter un lecteur USB :

1. Connectez une clé USB (avec l'image nécessaire) à la station de gestion.
2. Procédez comme suit pour lancer la console virtuelle via l'interface Web de l'iDRAC :
   - Accédez à **Tableau de bord** > **Console virtuelle** et cliquez sur **Lancer 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 la clé USB.
   L'image est ajoutée à la liste des lecteurs disponibles.
5. Sélectionnez le lecteur à lui associer. L'image sur la clé USB est associée au système géré.

Installation d'un système d'exploitation sur matériel vierge à l'aide d'un média virtuel connecté et du partage de fichier à distance

Voir la section Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance.

Gestion de la densité d'un rack

Avant d'installer des serveurs supplémentaires dans un rack, 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 de réseau de stockage SAN et que vous souhaitez leur appliquer différents paramètres d'adresse virtuelle, d'initiateur et de configuration cible, utilisez la fonctionnalité d'optimisation d'identité d'E/S pour réduire le temps de configuration des paramètres. Pour ce faire, procédez comme suit :

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 profil de configuration de serveur (SCP) à partir de l'iDRAC.
4. Modifiez les paramètres d'optimisation d'identité d'E/S dans le fichier SCP.
5. Importez le fichier SCP sur l'iDRAC.

Index

D

I