Guide de l'utilisateur de Integrated Dell Remote Access Controller 8 Version 2.70.70.70

September 2019
Rév. A00

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.

© 2019 Dell Inc. ou ses filiales. Tous droits réservés. Dell, EMC et les autres marques commerciales mentionnées sont des marques de Dell Inc. ou de ses filiales. Les autres marques peuvent être des marques commerciales de leurs propriétaires respectifs.

Table des matières

Chapitre 1: Présentation.....14
Avantages de l'utilisation d'iDRAC avec Lifecycle Controller.....14
Fonctions clés.....15
Nouveautés de cette version.....17
Utilisation du présent Guide d'utilisation.....17
Navigateurs web pris en charge.....18
Hyperviseurs et systèmes d'exploitation pris en charge.....18
Gérer les licences.....18
Types de licences.....18
Méthodes d'acquisition de licences.....18
Opérations de licence.....18
Fonctionnalités sous licence dans iDRAC7 et iDRAC8.....19
Interfaces et protocoles d'accès à iDRAC.....24
Informations sur les ports iDRAC.....26
Autres documents utiles.....27
Référence des médias sociaux.....28
Contacter Dell.....28
Accès aux documents à partir du site de support Dell EMC.....29

Chapitre 2: Ouverture de session dans iDRAC.....30
Ouverture de session dans iDRAC en tant qu'utilisateur local, utilisateur Active Directory ou utilisateur LDAP.....30
Connexion au contrôleur CMC avec une carte à puce.....31
Ouverture de session dans l'iDRAC en tant qu'utilisateur local à l'aide d'une carte à puce.....31
Ouverture de session dans l'iDRAC comme utilisateur Active Directory par carte à puce.....32
Ouverture d'une session iDRAC à l'aide de la connexion directe.....33
Ouverture d'une session dans iDRAC par connexion directe (SSO) à l'aide de l'interface Web iDRAC.....33
Ouverture d'une session dans l'iDRAC par la connexion directe (SSO) à l'aide de l'interface Web CMC.....33
Accès à l'iDRAC à l'aide de l'interface distante RACADM.....33
Validation d'un certificat d'autorité de certification (CA) pour utiliser l'interface distante RACADM sur Linux.....34
Accès à l'iDRAC à l'aide de l'interface locale RACADM.....34
Accès à l'iDRAC à l'aide de RACADM du micrologiciel.....34
Accès à l'iDRAC à l'aide de SMCLP.....34
Connexion à l'iDRAC à l'aide de l'authentification par clé publique.....34
Sessions iDRAC multiples.....35
Modification du mot de passe d'ouverture de session par défaut.....35
Modification du mot de passe d'ouverture de session par défaut à l'aide de l'interface web.....36
Modification du mot de passe d'ouverture de session par défaut à l'aide de RACADM.....36
Modification du mot de passe de connexion par défaut à l'aide de l'utilitaire Paramètres iDRAC.....36
Activation ou désactivation du message d'avertissement du mot de passe par défaut.....36
Activation ou désactivation du message d'avertissement de mot de passe par défaut à l'aide de l'interface Web.....37
Activation ou désactivation du message d'avertissement vous invitant à modifier le mot de passe d'ouverture de session par défaut à l'aide de RACADM.....37
Blocage d'adresse IP.....37

informations d'identification des mots de passe non valides....38

Chapitre 3: Installation du système géré et de la station de gestion....39
Définition de l'adresse IP d'iDRAC....39
Définition de l'adresse IP d'iDRAC à l'aide de l'utilitaire de configuration d'iDRAC....40
Définition de l'adresse IP d'iDRAC à l'aide de l'interface Web CMC....43
Activation du serveur de provisionnement....44
Configuration des serveurs et des composants du serveur à l'aide de la Configuration automatique....44
Utilisation des mots de passe cryptés pour une sécurité optimisée....50
Installation de la station de gestion....51
Accès à distance à l'iDRAC....51
Installation du système géré....51
Modification des paramètres du compte d'administrateur local....52
Définition de l'emplacement du système géré....52
Optimisation des performances du système et de la consommation d'énergie....53
Configuration des navigateurs web pris en charge....59
Configuration d'Internet Explorer....59
Configuration de Mozilla Firefox....60
Configuration des navigateurs Web pour utiliser la console virtuelle....60
Affichage des versions localisées de l'interface Web....64
Mise à jour du micrologiciel de périphérique....64
Mise à niveau du micrologiciel à l'aide de l'interface Web d'iDRAC....67
Mise à jour du micrologiciel de périphérique à l'aide de RACADM....69
Planification des mises à jour automatiques du micrologiciel....69
Mise à jour du micrologiciel à l'aide de l'interface Web CMC....71
Mise à jour du micrologiciel à l'aide de DUP....71
Mise à jour du micrologiciel à l'aide de l'interface RACADM....71
Mise à jour du micrologiciel à l'aide des Lifecycle Controller Remote Services....72
Mise à jour du micrologiciel CMC à partir de l'iDRAC....72
Affichage et gestion des mises à jour planifiées....73
Affichage et gestion des mises à jour intermédiaires à l'aide de l'interface Web d'iDRAC....73
Affichage et gestion des mises à jour différées à l'aide de RACADM....73
Restauration du micrologiciel du périphérique....73
Restauration du micrologiciel à l'aide de l'interface Web d'iDRAC....74
Restauration du micrologiciel à l'aide de l'interface Web CMC....75
Restauration du micrologiciel à l'aide de l'interface RACADM....75
Restauration du micrologiciel à l'aide du Lifecycle Controller....75
Restauration du micrologiciel à l'aide des services distants Lifecycle Controller....75
Restauration d'iDRAC....75
Utilisation du serveur TFTP....76
Sauvegarde du profil du serveur....76
Sauvegarde du profil du serveur à l'aide de l'interface Web iDRAC....76
Sauvegarde du profil du serveur à l'aide de RACADM....77
Planification de la sauvegarde automatique du profil de serveur....77
Importation du profil du serveur....78
Importation du profil du serveur à l'aide de l'interface Web iDRAC....79
Importation du profil du serveur à l'aide de RACADM....79
Séquence des opérations de restauration....79
Surveillance d'iDRAC à l'aide d'autres outils de gestion de systèmes....80

Chapitre 4: Configuration de l'iDRAC..... 81
Affichage des informations iDRAC.....82
Affichage des informations iDRAC à l'aide de l'interface Web..... 82
Affichage des informations iDRAC à l'aide de RACADM.....82
Modification des paramètres réseau.....82
Modification des paramètres réseau à l'aide de l'interface Web..... 83
Modification des paramètres réseau à l'aide de l'interface RACADM..... 83
Configuration du filtrage IP..... 83
Sélection des suites de chiffrement.....85
Configuration de la sélection des suites de chiffrement à l'aide de l'interface web iDRAC.....85
Configuration de la sélection des suites de chiffrement à l'aide de RACADM..... 85
Mode FIPS.....85
Activation du mode FIPS.....86
Désactivation du mode FIPS.....86
Configuration des services.....86
Configuration des services en utilisant l'interface web.....87
Configuration des services à l'aide de RACADM.....87
Activation ou désactivation de la redirection HTTPs.....87
Configuration de TLS.....88
Utilisation du client VNC pour gérer le serveur distant..... 88
Configuration de serveur VNC à l'aide de l'interface Web iDRAC..... 89
Configuration du serveur VNC à l'aide de RACADM..... 89
Configuration de VNC Viewer avec cryptage SSL.....89
Configuration de VNC Viewer sans cryptage SSL.....89
Configuration de l'écran du panneau avant..... 90
Configuration du paramétrage LCD..... 90
Configuration du paramétrage LED d'ID système.....91
Configuration du fuseau horaire et NTP..... 91
Configuration du fuseau horaire et du protocole NTP à l'aide de l'interface Web iDRAC..... 91
Configuration du fuseau horaire et du protocole NTP à l'aide de RACADM..... 92
Définition du premier périphérique de démarrage..... 92
Définition du premier périphérique de démarrage à l'aide de l'interface Web.....92
Définition du premier périphérique de démarrage à l'aide de RACADM.....93
Définition du premier périphérique de démarrage à l'aide de la console virtuelle..... 93
Activation du dernier écran de blocage..... 93
Activation ou désactivation de la connexion directe entre le SE et l'iDRAC.....93
Cartes prises en charge pour la connexion directe entre le système d'exploitation et l'iDRAC..... 94
Systèmes d'exploitation pris en charge pour la carte réseau USB.....95
Activation ou désactivation de la connexion directe à l'iDRAC à l'aide de l'interface Web..... 97
Activation ou désactivation de la connexion directe entre l'OS et l'iDRAC à l'aide de RACADM..... 97
Activation ou désactivation de la connexion directe à l'iDRAC à l'aide de l'utilitaire de paramètres iDRAC..... 97
Obtention de certificats.....98
Certificats de serveur SSL..... 99
Génération d'une nouvelle demande de signature de certificat.....100
Téléversement d'un certificat de serveur.....100
Affichage du certificat de serveur..... 101
Téléversement d'un certificat de signature personnalisée..... 101
Télécharger un certificat de signature de certificat SSL personnalisé 102
Suppression d'un certificat de signature de certificat SSL personnalisé..... 102

Configuration de plusieurs iDRAC à l'aide de RACADM....103
Création d'un fichier de configuration iDRAC....104
Désactivation de l'accès pour modifier les paramètres de configuration iDRAC sur un système hôte.... 104

Chapitre 5: Affichage des informations d'iDRAC et d'un système géré.... 105
Affichage de l'intégrité et des propriétés d'un système géré.... 105
Affichage de l'inventaire du système....106
Affichage des informations des capteurs....107
Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'E/S.... 108
Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'E/S via l'interface web....109
Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'E/S à l'aide de RACADM....109
Vérification de la conformité du système aux normes d'air frais.... 110
Affichage des données historiques de température.... 110
Affichage des données historiques de température à l'aide de l'interface Web iDRAC.... 110
Affichage des données historiques de température à l'aide de l'interface RACADM....111
Configuration du seuil d'avertissement de température d'entrée.... 111
Affichage des interfaces réseau disponibles sur le SE hôte....111
Affichage des interfaces réseau disponibles sur l'OS hôte à l'aide de l'interface web....112
Affichage des interfaces réseau disponibles sur l'OS hôte à l'aide de RACADM.... 112
Visualisation des connexions de structure des cartes mezzanines FlexAddress....112
Affichage ou fin des sessions iDRAC....113
Fin des sessions iDRAC à l'aide de l'interface Web.... 113
Fin des sessions iDRAC à l'aide de RACADM....113

Chapitre 6: Configuration de la communication iDRAC....114
Communication avec l'iDRAC via une connexion série à l'aide d'un câble DB9....115
Configuration du BIOS pour une connexion série....116
Activation d'une connexion série RAC.... 116
Activation des modes de base et terminal de connexion série IPMI.... 116
Permutation entre RAC Série et la console série à l'aide d'un câble DB9.... 118
Passage du mode console série au mode série RAC....118
Passage du mode RAC Série au mode Console série....118
Communication avec l'iDRAC à l'aide de SOL IPMI....119
Configuration du BIOS pour une connexion série....119
Configuration d'iDRAC pour utiliser SOL.... 119
Activation du protocole pris en charge.... 120
Communication avec l'iDRAC à l'aide d'IPMI sur LAN....124
Configuration d'IPMI sur LAN en utilisant l'interface Web....124
Configuration d'IPMI sur le LAN à l'aide de l'utilitaire de configuration d'iDRAC....125
Configuration d'IPMI sur le LAN à l'aide de RACADM.... 125
Activation ou désactivation de l'interface distante RACADM....125
Activation ou désactivation de l'interface distante RACADM à l'aide de l'interface web....126
Activation ou désactivation de l'interface RACADM distante à l'aide de RACADM....126
Désactivation de l'interface locale RACADM.... 126
Activation d'IPMI sur un système géré.... 126
Configuration de Linux pour la console série pendant le démarrage....126
Activation de l'ouverture de session dans la console virtuelle après le démarrage....127
Schémas cryptographiques SSH pris en charge....129

Utilisation de l'authentification par clé publique pour SSH..... 129

Chapitre 7: Configuration des comptes et des privilèges des utilisateurs..... 133
Caractères recommandés pour les noms d'utilisateur et mots de passe..... 133
Configuration des utilisateurs locaux..... 134
Configuration des utilisateurs locaux à l'aide de l'interface Web d'iDRAC..... 134
Configuration des utilisateurs locaux à l'aide de RACADM..... 134
Configuration des utilisateurs d'Active Directory..... 136
Exigences d'utilisation de l'authentification Active Directory pour l'iDRAC..... 137
Mécanismes d'authentification Active Directory pris en charge..... 139
Présentation d'Active Directory avec le schéma standard..... 139
Configuration d'Active Directory avec le schéma standard..... 140
Présentation d'Active Directory avec schéma étendu..... 142
Configuration du schéma étendu Active Directory..... 144
Test des paramètres Active Directory..... 152
Configuration d'utilisateurs LDAP générique..... 153
Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web d'iDRAC..... 153
Configuration du service d'annuaire LDAP générique à l'aide de RACADM..... 154
Test des paramètres du service d'annuaire LDAP..... 154

Chapitre 8: Configuration de l'iDRAC pour la connexion directe ou par carte à puce..... 155
Exigences d'ouverture de session Active Directory par connexion directe ou carte à puce..... 155
Enregistrement d'iDRAC en tant qu'ordinateur dans un domaine racine Active Directory..... 156
Génération d'un fichier Keytab Kerberos..... 156
Création d'objets Active Directory et fourniture de privilèges..... 156
Configuration d'ouverture de session par connexion directe (SSO) iDRAC pour les utilisateurs Active Directory..... 157
Configuration d'ouverture de session dans l'iDRAC par connexion directe (SSO) pour les utilisateurs Active Directory à l'aide de l'interface Web..... 157
Configuration d'ouverture de session iDRAC par connexion directe (SSO) pour les utilisateurs Active Directory à l'aide de RACADM..... 157
Configuration d'ouverture de session iDRAC par carte à puce pour les utilisateurs locaux..... 158
Téléversement du certificat d'utilisateur de carte à puce..... 158
Téléversement d'un certificat d'autorité de certification pour une carte à puce..... 158
Configuration de la connexion par carte à puce iDRAC pour les utilisateurs Active Directory..... 159
Activation ou désactivation de l'ouverture de session par carte à puce..... 159
Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de l'interface Web..... 160
Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de l'interface RACADM..... 160
Activation ou désactivation de l'ouverture de session par carte à puce à l'aide de l'utilitaire de configuration d'iDRAC..... 160

Chapitre 9: Configuration d'iDRAC pour envoyer des alertes..... 161
Activation ou désactivation des alertes..... 162
Activation ou désactivation des alertes à l'aide de l'interface Web..... 162
Activation ou désactivation des alertes à l'aide de RACADM..... 162
Activation ou désactivation des alertes à l'aide de l'utilitaire de configuration iDRAC..... 162
Filtrage des alertes..... 162
Filtrage des alertes à l'aide de l'interface Web iDRAC..... 162
Filtrage des alertes à l'aide de l'interface RACADM..... 163
Définition d'alertes d'événement..... 163

Définition d'alertes d'événements à l'aide de l'interface Web....163
Définition d'alertes d'événement à l'aide de l'interface RACADM....164
Définition d'événement de récurrence d'alerte....164
Définition d'événements de récurrence d'alerte à l'aide de l'interface Web iDRAC....164
Définition d'événements de récurrence d'alerte à l'aide de l'interface RACADM....164
Définition d'actions d'événement....164
Définition d'actions d'événement à l'aide de l'interface Web....164
Définition d'actions d'événements à l'aide de l'interface RACADM....165
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI....165
Configuration des destinations d'alerte IP....165
Configuration des paramètres d'alerte par e-mail....167
Configuration des événements WS....168
Configuration des événements Redfish....169
Surveillance des événements de châssis....169
Surveillance des événements du châssis à l'aide de l'interface Web iDRAC....169
Surveillance des événements du châssis à l'aide de RACADM....169
ID de message d'alerte....170

Chapitre 10: Gestion des journaux....173
Affichage du journal des événements système....173
Affichage du journal des événements système à l'aide de l'interface Web....173
Affichage du journal des événements système à l'aide de l'interface RACADM....174
Affichage du journal des événements système à l'aide de l'utilitaire de configuration d'iDRAC....174
Affichage du journal Lifecycle....174
Affichage du journal Lifecycle à l'aide de l'interface Web....175
Affichage du journal Lifecycle à l'aide de l'interface RACADM....175
Exportation des journaux du Lifecycle Controller....175
Exportation des journaux du Lifecycle Controller à l'aide de l'interface Web....175
Exportation des journaux Lifecycle Controller via RACADM....176
Ajout de notes de travail....176
Configuration de la journalisation d'un système distant....176
Configuration de la journalisation d'un système distant à l'aide de l'interface Web....176
Configuration de la journalisation du système distant à l'aide de RACADM....177

Chapitre 11: Surveillance et gestion de l'alimentation....178
Surveillance de l'alimentation....178
Surveillance de l'alimentation à l'aide de l'interface Web....178
Surveillance de l'alimentation à l'aide de RACADM....179
Définition du seuil d'avertissement de consommation d'alimentation....179
Définition du seuil d'avertissement de consommation d'énergie à l'aide de l'interface Web....179
Exécution d'opérations de contrôle de l'alimentation....179
Exécution des opérations de contrôle de l'alimentation à l'aide de l'interface Web....179
Exécution d'opérations de contrôle de l'alimentation à l'aide de l'interface RACADM....180
Plafonnement de l'alimentation....180
Limitation de la puissance dans les serveurs lames....180
Affichage et configuration d'une stratégie de limitation de puissance....180
Configuration des options d'alimentation....181
Configuration des options d'alimentation à l'aide de l'interface Web....182
Configuration des options d'alimentation électrique à l'aide de l'interface RACADM....182

Configuration des options d'alimentation à l'aide de l'utilitaire de configuration d'iDRAC.....182
Activation ou désactivation du bouton d'alimentation.....183

Chapitre 12: Configuration, surveillance et inventaire des périphériques réseau.....184
Inventaire et surveillance des périphériques réseau.....184
Surveillance des périphériques réseau à l'aide de l'interface Web.....184
Surveillance des périphériques réseau à l'aide de RACADM.....185
Inventaire et surveillance des périphériques HBA FC.....185
Surveillance des périphériques HBA FC à l'aide de l'interface Web.....185
Surveillance des périphériques HBA FC à l'aide de RACADM.....185
Configuration dynamique des adresses virtuelles, de l'initiateur et de la cible de stockage.....185
Cartes prises en charge pour l'optimisation d'identité d'E/S.....186
Versions du micrologiciel des cartes réseau prises en charge pour l'optimisation de l'identité des E/S.....187
Comportement de Virtual ou Flex Address et de la stratégie de persistance lorsque le contrôleur iDRAC est défini sur le mode Console ou Flex Address.....187
Comportement du système pour l'identité d'E/S et FlexAddress.....189
Activation ou désactivation de l'optimisation d'identité d'E/S.....189
Configuration des paramètres de la stratégie de persistance.....190

Chapitre 13: Gestion de périphériques de stockage.....194
Présentation des concepts RAID.....195
RAID.....196
Organisation du stockage des données à des fins de disponibilité et de performances.....197
Choix des niveaux de RAID.....197
Comparaison des performances des niveaux RAID.....203
Contrôleurs pris en charge.....204
Boîtiers pris en charge.....205
Récapitulatif des fonctions prises en charge pour les périphériques de stockage.....205
Inventaire et surveillance des périphériques de stockage.....207
Surveillance des périphériques de stockage à l'aide de l'interface Web.....208
Surveillance d'un périphérique de stockage à l'aide de l'interface RACADM.....208
Surveillance d'un fond de panier à l'aide de l'utilitaire de paramètres d'iDRAC.....208
Affichage de la topologie des périphériques de stockage.....208
Gestion des disques physiques.....208
Affectation ou annulation de l'affectation d'un disque physique comme disque de secours global.....209
Conversion d'un disque physique au mode RAID ou non RAID.....210
Gestion de disques virtuels.....211
Création de disques virtuels.....211
Modification des règles de cache des disques virtuels.....213
Suppression de disques virtuels.....213
Vérification de cohérence de disque virtuel.....214
Initialisation des disques virtuels.....214
Chiffrement de disques virtuels.....215
Affectation ou annulation de l'affectation de disques de secours dédiés.....215
Gestion de disques virtuels à l'aide de l'interface web.....215
Gestion de disques virtuels à l'aide de RACADM.....216
Gestion des contrôleurs.....217
Configuration des propriétés du contrôleur.....217
Importation ou importation automatique d'une configuration étrangère.....220
Suppression d'une configuration étrangère.....221

Réinitialisation de la configuration d'un contrôleur....222
Basculement de mode de contrôleur....222
Opérations de l'adaptateur HBA SAS 12 Gbits/s....224
Surveillance de l'analyse de la prédiction d'échec sur des disques....224
Opérations de contrôleur en mode non RAID - HBA....224
Exécution de tâches de configuration RAID sur plusieurs contrôleurs de stockage....225
Gestion des SSD PCIe....225
Inventaire et surveillance de SSD PCIe....226
Préparation au retrait d'un SSD PCIe....226
Effacement des données d'un périphérique SSD PCIe....228
Gestion des boîtiers ou des fonds de panier....229
Configuration du mode du fond de panier....229
Affichage des logements universels....232
Définition du mode SGPIO....232
Choix du mode de fonctionnement pour l'application des paramètres....233
Choix du mode de fonctionnement à l'aide de l'interface Web....233
Choix du mode de fonctionnement à l'aide de RACADM....234
Affichage et application des opérations en attente....234
Affichage, application ou suppression des opérations en attente à l'aide de l'interface Web....234
Affichage et application des opérations en attente à l'aide de RACADM....235
Périphériques de stockage : scénarios d'opérations d'application....235
Clignotement ou annulation du clignotement des LED des composants....236
Faire clignoter ou arrêter le clignotement des LED des composants à l'aide de l'interface Web....236
Clignotement ou annulation du clignotement des LED des composants à l'aide de RACADM....237

Chapitre 14: Configuration et utilisation de la console virtuelle....238
Résolutions d'écran prises en charge et taux de rafraîchissement correspondants....238
Configuration de la console virtuelle....239
Configuration de la console virtuelle à l'aide de l'interface web....239
Configuration de la console virtuelle à l'aide de l'interface RACADM....239
Prévisualisation de la console virtuelle....239
Lancement de la console virtuelle....240
Lancement de la console virtuelle à l'aide de l'interface Web....240
Lancement de la console virtuelle à l'aide d'une URL....240
Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX....241
Utilisation du Visualiseur de console virtuelle....241
Console virtuelle HTML5....242
Synchronisation des pointeurs de souris....243
Envoi de toutes les frappes de touches via la console virtuelle pour le plug-in Java ou ActiveX....244

Chapitre 15: Gestion de Média Virtuel....247
Lecteur et périphériques pris en charge....248
Configuration de média virtuel....248
Configuration de média virtuel à l'aide de l'interface Web d'iDRAC....248
Configuration de média virtuel à l'aide de RACADM....248
Configuration de Média Virtuel à l'aide de l'utilitaire de configuration d'iDRAC....248
État de média connecté et réponse du système....249
Accès à un média virtuel....249
Lancement de Média Virtuel à l'aide de la console virtuelle....249

Lancement de Média Virtuel sans utiliser la console virtuelle....250
Ajout d'images Média Virtuel....250
Affichage des informations détaillées d'un périphérique virtuel....251
Réinitialisation USB....251
Mappage d'un lecteur virtuel....251
Dissociation d'un lecteur virtuel....252
Définition de la séquence de démarrage via le BIOS....253
Activation du démarrage unique pour Média Virtuel....253

Chapitre 16: Installation et utilisation de l'utilitaire VMCLI....254
Installation de VMCLI....254
Exécution de l'utilitaire VMCLI....254
Syntaxe VMCLI....254
Commandes VMCLI pour accéder à Média Virtuel....255
Options shell de système d'exploitation WMCLI....255

Chapitre 17: Gestion de la carte SD vFlash....257
Configuration d'une carte SD vFlash....257
Affichage des propriétés d'une carte SD vFlash....257
Activation ou désactivation de la fonctionnalité vFlash....258
Initialisation d'une carte SD vFlash....259
Obtention du dernier état à l'aide de RACADM....259
Gestion des partitions vFlash....260
Création d'une partition vide....260
Création d'une partition à l'aide d'un fichier image....261
Formatage d'une partition....262
Affichage des partitions disponibles....262
Modification d'une partition....263
Connexion et déconnexion de partitions....263
Suppression de partitions existantes....264
Téléchargement du contenu d'une partition....265
Démarrage à partir d'une partition....265

Chapitre 18: Utilisation de SMCLP....267
Fonctions de gestion de système à l'aide de SMCLP....267
Exécution des commandes SMCLP....267
Syntaxe SMCLP iDRAC....268
Navigation dans l'espace d'adressage MAP....271
Utilisation du verbe show....271
Utilisation de l'option -display....271
Utilisation de l'option -level....271
Utilisation de l'option -output....272
Exemples d'utilisation....272
Gestion de l'alimentation du serveur....272
Gestion du journal SEL....272
Navigation dans la cible MAP....274

Chapitre 19: Utilisation de l'iDRAC Service Module....275
Installation de l'iDRAC Service Module....275

Systèmes d'exploitation pris en charge de l'iDRAC Service Module..... 275
Fonctionnalités de surveillance de l'iDRAC Service Module..... 276
Utilisation de l'iDRAC Service Module à partir de l'interface Web iDRAC..... 282
Utilisation de l'iDRAC Service Module à l'aide de RACADM..... 283
Utilisation d'iDRAC Service Module d'iDRAC sur Windows Nano..... 283

Chapitre 20: Utilisation d'un port USB pour la gestion de serveur..... 284
Accès à l'interface iDRAC via connexion USB directe..... 284
Configuration de l'iDRAC à l'aide du profil de configuration de serveur sur un périphérique USB..... 285
Configuration des paramètres du port de gestion USB..... 285
Importation du profil de configuration de serveur depuis un périphérique USB..... 287

Chapitre 21: Utilisation de la fonction Quick Sync (Synchronisation rapide) d'iDRAC..... 289
Configuration de la fonction Quick Sync (Synchronisation rapide) d'iDRAC..... 289
Configuration des paramètres de la fonction Quick Sync (Synchronisation rapide) d'iDRAC à l'aide de l'interface Web..... 290
Configuration des paramètres de la fonction Quick Sync (Synchronisation rapide) d'iDRAC à l'aide de RACADM..... 290
Configuration des paramètres de la fonction Quick Sync (Synchronisation rapide) d'iDRAC à l'aide de l'utilitaire de configuration d'iDRAC..... 290
Utilisation d'un appareil mobile pour afficher des informations sur iDRAC..... 291

Chapitre 22: Déploiement de systèmes d'exploitation..... 292
Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance..... 292
Gestion du partage de fichier à distance..... 292
Configuration du partage de fichier à distance à l'aide de l'interface web..... 293
Configuration du partage de fichier à distance à l'aide de RACADM..... 294
Déploiement d'un système d'exploitation à l'aide de Média Virtuel..... 294
Installation d'un système d'exploitation depuis plusieurs disques..... 295
Déploiement d'un système d'exploitation intégré sur une carte SD..... 295
Activation du module SD et de la redondance dans le BIOS..... 295

Chapitre 23: Dépannage d'un système géré à l'aide d'iDRAC..... 297
Utilisation de la console de diagnostic..... 297
Planification de diagnostics automatisés à distance..... 298
Planification des diagnostics automatisés à distance à l'aide de RACADM..... 298
Affichage des codes du Post..... 299
Affichage des vidéos de capture de démarrage et de blocage..... 299
Configuration des paramètres de capture vidéo..... 299
Affichage des journaux..... 299
Affichage de l'écran du dernier blocage du système..... 300
Affichage de l'état du panneau avant..... 300
Affichage de l'état du panneau avant LCD..... 300
Affichage de l'état LED du panneau avant du système..... 300
Voyants des problèmes matériels..... 301
Affichage de l'intégrité du système..... 301
Génération de la collecte SupportAssist..... 302
Génération automatique de la collecte pour SupportAssist..... 303
Génération manuelle de la collecte SupportAssist..... 303
Vérification des messages d'erreur dans l'écran d'état du serveur..... 305

Redémarrage d'iDRAC....305
Réinitialisation d'iDRAC à l'aide de l'interface Web iDRAC....305
Réinitialisation d'iDRAC à l'aide de l'interface RACADM....305
Effacement des données système et utilisateur....305
Restauration des paramètres par défaut définis en usine d'iDRAC....306
Restauration des paramètres par défaut définis en usine d'iDRAC à l'aide de l'interface Web iDRAC....306
Restauration des paramètres par défaut définis en usine d'iDRAC à l'aide de l'utilitaire de Configuration d'iDRAC....306

Chapitre 24: Questions fréquemment posées....307
Journal des événements système....307
Sécurité du réseau....308
Active Directory....308
Connexion directe....310
Ouverture de session avec une carte à puce....311
Console virtuelle....311
Média virtuel....314
Carte SD vFlash....316
Authentification SNMP....316
Périphériques de stockage....316
iDRAC Service Module....316
RACADM....318
Divers....319

Chapitre 25: Scénarios de cas d'utilisation....322
Dépannage d'un système géré inaccessible....322
Obtention des informations système et évaluation de l'intégrité du système....323
Définition des alertes et configuration des alertes par e-mail....323
Affichage et exportation du journal Lifecycle et du journal des événements système....323
Interfaces de mise à niveau du micrologiciel iDRAC....323
Exécution d'un arrêt normal....324
Création d'un compte utilisateur Administrateur....324
Lancement de la console distante du serveur et montage d'un lecteur USB....324
Installation d'un système d'exploitation nu à l'aide d'un média virtuel connecté et du partage de fichier à distance....324
Gestion de la densité d'un rack....325
Installation d'une nouvelle licence électronique....325
Application des paramètres de configuration d'identité d'E/S pour plusieurs cartes réseau lors du redémarrage d'un système hôte unique....325

1

Présentation

Le contrôleur d'accès à distance Dell intégré (iDRAC, Integrated Dell Remote Access Controller) est conçu pour accroître la productivité des administrateurs de serveurs et améliorer la disponibilité générale des serveurs Dell. iDRAC alerte les administrateurs en cas de problème avec le serveur, leur permet de gérer ce dernier à distance et réduit la nécessité d'y accéder physiquement.

Le contrôleur iDRAC, avec la technologie Lifecycle Controller, fait partie d'une vaste solution de datacenter qui permet d'assurer la disponibilité des applications et charges applicatives stratégiques. Avec cette technologie, les administrateurs peuvent déployer, surveiller, gérer, configurer, mettre à jour, dépanner et réparer les serveurs Dell depuis tout emplacement et sans agent. Ces opérations sont possibles, qu'un système d'exploitation ou un hyperviseur soit présent ou non, ou quel que soit l'état du système d'exploitation ou de l'hyperviseur.

Plusieurs produits fonctionnent avec l'iDRAC et le Lifecycle Controller pour simplifier et rationaliser les opérations informatiques :

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

Il existe les variantes suivantes d'iDRAC :

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

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

Sujets :

- Avantages de l'utilisation d'iDRAC avec Lifecycle Controller
- Fonctions clés
- Nouveautés de cette version
- Utilisation du présent Guide d'utilisation
- Navigateurs web pris en charge
- Hyperviseurs et systèmes d'exploitation pris en charge
- Gérer les licences
- Fonctionnalités sous licence dans iDRAC7 et iDRAC8
- Interfaces et protocoles d'accès à iDRAC
- Informations sur les ports iDRAC
- Autres documents utiles
- Référence des médias sociaux
- Contacter Dell
- Accès aux documents à partir du site de support Dell EMC

Avantages de l'utilisation d'iDRAC avec Lifecycle Controller

Avantages :

- Amélioration de la disponibilité : notification anticipée des échecs potentiels ou réels pour empêcher la défaillance d'un serveur ou réduire le temps de récupération après un incident.

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

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

Fonctions clés

Principales fonctions disponibles dans iDRAC :

REMARQUE : Certaines fonctions sont disponibles uniquement sous licence iDRAC Enterprise. Pour plus d'informations sur les fonctions disponibles avec une licence, voir Gestion des licences.

Inventaire et surveillance

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

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

- Affichez les interfaces réseau disponibles sur les systèmes d'exploitation hôtes.
- Affichez des informations d'inventaire et de surveillance et configuration des paramètres iDRAC de base à l'aide de la fonction Quick Sync (Synchronisation rapide) d'iDRAC et un appareil mobile.

Déploiement

- Gestion des partitions de carte SD vFlash SD
- Configuration des paramètres de l'écran du panneau avant
- Gestion des paramètres réseau iDRAC.
- Configuration et utilisation d'une console virtuelle de média virtuel
- Déploiement de systèmes d'exploitation en utilisant le partage de fichier à distance, média virtuel et VMCLI.
- Activation de l'auto-détection.
- Effectuez la configuration du serveur à l'aide de la fonction d'exportation ou d'importation du profil XML via RACADM et WSMAN. Pour plus d'informations, voir le *Lifecycle Controller Remote Services Quick Start Guide* (disponible en anglais uniquement).
- Configurez la règle 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 d'un 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 de périphérique 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.

Mettre à jour

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

Maintenance et dépannage

- Exécution d'opérations d'alimentation et surveillance de la consommation d'énergie.
- Optimisez les performances du système et la consommation d'énergie en modifiant les paramètres thermiques.
- Aucune dépendance de l'administrateur de serveur pour la génération d'alertes.
- 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 l'UC, la mémoire et les modules d'E/S.
- Configurer le seuil d'avertissement de la température d'entrée et de la consommation d'énergie.
- 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.
    - Hard-reset de l'iDRAC à distance
    - Alertes SNMP intrabande de l'iDRAC
    - Accéder à l'iDRAC à l'aide de l'OS hôte (fonctionnalité expérimentale)
    - Entrée des informations Windows Management Instrumentation (WMI).
    - Intégration à la collection SupportAssist. Cela s'applique uniquement si l'iDRAC Service Module version 2.0 ou ultérieure est installé. Pour plus d'informations, voir Générer la collecte SupportAssist).
    - Préparation au retrait d'une carte SSD PCIe NVMe Pour plus d'informations, voir Préparation au retrait d'un SSD PCIe , page 226.
- Génération de la collecte pour SupportAssist de l'une des manières suivantes :
    - Automatique : utilisation du Service module d'iDRAC qui appelle automatiquement l'outil OS Collector.
    - Manuel : utilisation de l'outil de collecte de l'OS

Les meilleures pratiques de Dell concernant iDRAC

- Les iDRAC sont conçus pour figurer sur un réseau de gestion distinct ; ils ne sont pas destinés à être placés sur Internet ou connectés 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.
- En plus de placer les iDRAC 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

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

- Certificat de signature personnalisé pour le certificat SSL (couche de sockets sécurisée).
- Mises à jour signées du micrologiciel
- Authentification utilisateur via Microsoft Active Directory, service de répertoire LDAP (Lightweight Directory Access Protocol - Protocole d'accès aux annuaires allégé) générique, ou ID et mots de passe utilisateur administrés localement.
- Authentification à deux facteurs utilisant la fonction de connexion par carte à puce. Cette authentification repose sur la carte à puce physique et son code PIN.
- Connexion directe et authentification par clé publique.
- Autorisation basée sur le rôle pour définir des privilèges pour chaque utilisateur
- 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 la référence 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 crypté unidirectionnel pour une sécurité renforcée.
- Capacité FIPS 140-2 de niveau 1.
- Prise en charge de TLS 1.2, 1.1 et 1.0. Pour optimiser la sécurité, le paramètre par défaut est TLS 1.1 et version supérieure.
- Interfaces SMCLP et web prenant en charge le cryptage 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté) à l'aide de la norme TLS 1.2

REMARQUE : Pour assurer une connexion sécurisée, Dell recommande d'utiliser TLS 1.1 et plus récent.

- Configuration du délai d'expiration de la session (en secondes)
- Ports IP configurables (pour HTTP, HTTPS, SSH, Telnet, la console virtuelle et Média Virtuel).

  REMARQUE : Telnet ne prend pas en charge le chiffrement SSL et il est désactivé par défaut
- SHH (Secure Shell) qui utilise une couche de transport cryptée pour une sécurité accrue.
- Nombre maximal d'échecs de connexion par adresse IP, avec blocage de connexion à partir de cette adresse IP lorsque la limite est dépassée
- Plage d'adresses IP limitée pour les clients se connectant à iDRAC.
- Adaptateur de la carte Gigabit Ethernet dédiée disponible sur les serveurs en rack et de type tour (du matériel supplémentaire peut être requis).

Nouveautés de cette version

- Ajout de la prise en charge de la mise à jour de firmware des disques SSD Intel P4510 et P4610.
- Ajout de la prise en charge de la mise à jour de firmware des appareils iDSDM.
- Ajout de la prise en charge de la mise à jour de firmware via HTTPS.
- Ajout de la prise en charge de l'adresse IPv6 pour USB-NIC pour prendre en charge la connexion directe du système d'exploitation.
- Ajout de la prise en charge de PSU-56 et de CSDM-53.
- Suppression de l'URL par défaut de l'option Paramètres du serveur FTP.
- URL par défaut de la page HTTPS : downloads.dell.com.

Utilisation du présent Guide d'utilisation

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

- 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*, qui est accessible via l'interface web.
- RACADM : la commande RACADM ou l'objet que vous devez utiliser sont fournis ici. Pour en savoir plus, voir le *iDRAC RACADM Command Line Reference Guide (Guide de référence de la ligne de commande RACADM iDRAC)*, disponible sur **dell.com/idracmanuals**.
- L'utilitaire de configuration d'iDRAC : seules les informations liées aux tâches sont fournies ici. Pour des informations concernant les champs et les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*, accessible en cliquant sur **Help (Aide)** dans l'interface graphique des paramètres d'iDRAC (appuyez sur <F2> lors du démarrage, puis cliquez sur **iDRAC Settings (Paramètres iDRAC)** à la page **System Setup Main Menu (Menu principal de configuration du système)**.

Navigateurs web pris en charge

iDRAC est pris en charge sur les navigateurs suivants :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Pour consulter la liste des versions prises en charge, voir le fichier *iDRAC Notes de mise à jour d'iDRAC* , disponible sur **dell.com/idracmanuals**.

Hyperviseurs et systèmes d'exploitation pris en charge

iDRAC est pris en charge sur les hyperviseurs et systèmes d'exploitation suivants :

- Microsoft
- VMware
- Citrix
- RedHat
- SuSe

REMARQUE : Pour consulter la liste des versions prises en charge, voir le fichier *iDRAC Notes de mise à jour d'iDRAC* , disponible sur **dell.com/idracmanuals**.

Gérer les licences

Les fonctionnalités d'iDRAC sont disponibles en fonction de la licence achetée (Gestion de base, iDRAC Express ou iDRAC Enterprise). Seules les fonctions sous licence sont disponibles dans les interfaces qui permettent de configurer ou d'utiliser iDRAC. Par exemple, l'interface web iDRAC, RACADM, WSMAN, OpenManage Server Administrator, et ainsi de suite. Certaines fonctionnalités, telles que NIC ou vFlash, nécessitent une carte de ports iDRAC. Cette dernière est disponible en option sur les serveurs de série 200 à 500.

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

Types de licences

Les types de licences proprosés 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 au numéro de service et elle est prermanente.

Méthodes d'acquisition de licences

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

- E-mail : la licence est jointe à un e-mail envoyé après sa demande auprès du centre d'assistance technique.
- Dell Digital Locker : un lien vers Dell Digital Locker est disponible dans l'interface utilisateur de l'iDRAC. Cliquez sur ce lien pour ouvrir le portail des licences sur Internet. Pour le moment, vous pouvez utiliser Dell Digital Locker pour récupérer les licences achetées avec le serveur. Vous devez contacter l'ingénieur commercial ou le support technique pour acheter une licence nouvelle ou de mise à niveau. Pour plus d'informations, voir la section FAQ sur la page Dell Digital Locker.
- Point de vente : la licence est acquise lors de la commande d'un système.

Opérations de licence

Avant d'exécuter les tâches de gestion des licences, veillez à obtenir les licences. Pour en savoir plus, voir le *Guide de présentation et des fonctions iDRAC* disponible à l'adresse **dell.com/support/manuals**.

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

Vous pouvez exécuter les opérations de licence suivantes en utilisant iDRAC, RACADM, WSMAN 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 : Pour un nombre limité de fonctions, il est nécessaire de redémarrer le système pour activer les fonctions.

- Exporter : exporter la licence installée sur un dispositif de stockage externe pour disposer d'une sauvegarde, ou la réinstaller après le remplacement d'un composant ou de la carte mère. Nom de fichier et format de la licence exportée : **<IDpropriété>.xml**.
- Supprimer : supprimer la licence attribuée à un composant manquant. Une fois supprimée, la licence n'est plus stockée dans l'iDRAC et les fonctions de base du produit sont activées.
- Remplacer : changer un type de licence (remplacement d'une licence d'évaluation par une licence achetée) ou étendre une licence expirée.
  - Une licence d'évaluation peut être remplacée par une licence d'évaluation mise à niveau ou une licence achetée.
  - Une licence achetée peut être remplacée par une licence mise à niveau ou une licence mise à jour.
- En savoir plus : en savoir plus sur une licence installée ou les licences disponibles pour un composant installé sur le serveur.

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

Pour le déploiement de licence un à plusieurs, vous pouvez utiliser Dell License Manager. Pour obtenir des informations complètes, voir le *Guide d'utilisation du Gestionnaire de licences Dell* disponible sur **dell.com/support/manuals**.

Importation de la licence suite au remplacement de la carte mère

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

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

Pour gérer les licences à l'aide de l'interface web d'iDRAC, accédez à **Présentation** > **Serveur** > **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, la suppression ou le remplacement d'une licence, voir l'*Aide en ligne d'iDRAC*.

REMARQUE : Dans l'interface web d'iDRAC, sur la page **Licences**, développez l'appareil afin de voir l'option **Remplacer** dans le menu déroulant **Options de licence**.

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

Pour gérer les licences à l'aide de l'interface RACADM, utilisez la sous-commande **licence**. Pour en savoir plus, voir l'*iDRAC RACADM Command Line Interface Reference Guide* (Guide de référence de l'interface de ligne de commande RACADM iDRAC) disponible à l'adresse **dell.com/idracmanuals**.

Fonctionnalités sous licence dans iDRAC7 et iDRAC8

Le tableau suivant répertorie les fonctions iDRAC7 et iDRAC8 activées en fonction de la licence achetée :

Tableau 1. Fonctionnalités sous licence dans iDRAC7 et iDRAC8

Fonctionnalité	Gestion de base (iDRAC 7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express pour lames	iDRAC8 Express pour lames	iDRAC7 Enterprise	iDRAC8 Enterprise
Interfaces/normes								
IPMI 2.0	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
DCMI 1.5	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Interface utilisateur graphique Web	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Ligne de commande RACADM (local/à distance)	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Redfish	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
SMASH-CLP (SSH-only)	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Telnet	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
SSH	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
WSMAN	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
NTP (Protocole de temps du réseau)	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Connectivité								
Carte d'interface réseau partagée (LOM)	Oui	Oui	Oui	Oui	S/O	S/O	Oui	Oui
NIC[1] dédiée	Non	Oui	Non	Oui	Oui	Oui	Oui	Oui[2]
Marquage VLAN	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
IPv4	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
IPv6	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
DHCP	Non	Oui	Non	Oui	Non	Oui	Non	Oui
DNS dynamique	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Connexion directe de l'OS	Non	Oui	Non	Oui	Non	Oui	Non	Oui
USB du panneau avant	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Sécurité								
Autorité basée sur les rôles	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Utilisateurs locaux	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Chiffrement SSL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Blocage d'adresse IP	Non	Non	Non	Oui	Non	Oui	Non	Oui
Services de répertoire (AD, LDAP)	Non	Non	Non	Non	Non	Non	Oui	Oui
L'authentification à deux facteurs (carte à puce)	Non	Non	Non	Non	Non	Non	Oui	Oui
Accès avec connexion unique (kerberos)	Non	Non	Non	Oui	Non	Oui	Oui	Oui

Tableau 1. Fonctionnalités sous licence dans iDRAC7 et iDRAC8 (suite)

Fonctionnalité	Gestion de base (iDRAC 7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express pour lames	iDRAC8 Express pour lames	iDRAC7 Enterprise	iDRAC8 Enterprise
Authentification PK (pour SSH)	Non	Non	Non	Oui	Non	Oui	Non	Oui
Présence à distance								
Bouton d'alimentation	Oui[4]	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Contrôle de l'amorçage	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Série sur LAN	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Virtual Media	Non	Non	Non	Non	Oui	Oui	Oui	Oui
Dossiers virtuels	Non	Non	Non	Non	Non	Non	Oui	Oui
Partage de fichier à distance	Non	Non	Non	Non	Non	Non	Oui	Oui
Console virtuelle	Non	Non	Non	Non	Utilisateur unique	Utilisateur unique	Oui	6 utilisateurs
Connexion VNC à l'OS	Non	Non	Non	Non	Non	Non	Oui	Oui
Contrôle de la qualité/ bande passante	Non	Non	Non	Non	Non	Oui	Non	Oui
Collaboration de console virtuelle (jusqu'à six utilisateurs simultanés)	Non	Non	Non	Non	Non	Non	Non	Oui
Chat console virtuelle	Non	Non	Non	Non	Non	Non	Oui	Oui
Partitions Virtual Flash	Non	Non	Non	Non	Non	Non	Oui	Oui [1,2]
Alimentation et Thermique								
Mise sous tension automatique après une perte	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Mesure d'énergie en temps réel	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Seuils d'alimentation et alertes (y compris seuil de marge)	Non	Non	Non	Oui	Non	Oui	Non	Oui
Graphique d'alimentation en temps réel	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Compteurs d'alimentation historiques	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui
Limitation de l'alimentation	Non	Non	Non	Non	Non	Non	Oui	Oui
Intégration de Power Center	Non	Non	Non	Non	Non	Non	Non	Oui
Surveillance de la température	Non	Oui	Non	Oui	Non	Oui	Non	Oui

Tableau 1. Fonctionnalités sous licence dans iDRAC7 et iDRAC8 (suite)

Fonctionnalité	Gestion de base (iDRAC 7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express pour lames	iDRAC8 Express pour lames	iDRAC7 Enterprise	iDRAC8 Enterprise
Graphiques de température	Non	Non	Non	Oui	Non	Oui	Non	Oui
Surveillance de l'intégrité								
Surveillance sans agent complète	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance de panne prédictive	Non	Oui	Non	Oui	Non	Oui	Non	Oui
SNMP v1, v2 et v3 (interruptions et gets)	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Alertes par e-mail	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Seuils configurables	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance du ventilateur	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance des blocs d'alimentation	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Surveillance de la mémoire	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance du processeur	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance de RAID	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance de NIC	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance de HD (boîtier)	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance des performances hors bande	Non	Non	Non	Non	Non	Non	Non	Oui
Mettre à jour								
Mise à jour sans agent à distance	Oui[3]	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Outils de mise à jour intégrés	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Synchroniser avec une logithèque (mises à jour planifiées)	Non	Non	Non	Non	Non	Non	Oui	Oui
Mise à jour automatique	Non	Non	Non	Non	Non	Non	Non	Oui
Déploiement et configuration								

Tableau 1. Fonctionnalités sous licence dans iDRAC7 et iDRAC8 (suite)

Fonctionnalité	Gestion de base (iDRAC 7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express pour lames	iDRAC8 Express pour lames	iDRAC7 Enterprise	iDRAC8 Enterprise
Outils intégrés de déploiement de l'OS	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Outils de configuration intégrés (utilitaire de paramètres d'iDRAC)	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Assistants Configuration intégrés (Assistants Lifecycle Controller)	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Détection automatique	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Déploiement de l'OS à distance	Non	Non	Non	Oui	Non	Oui	Non	Oui
Pack de pilotes intégré	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Inventaire de configuration complet	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Exportation de l'inventaire	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Configuration à distance	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Configuration sans intervention	Non	Non	Non	Non	Non	Non	Non	Oui
Système hors service/ recyclé	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Diagnostics, Service et Journalisation								
Outils de diagnostic intégrés	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Remplacement de pièce	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Sauvegarde de la configuration du serveur	Non	Non	Non	Non	Non	Non	Oui	Oui
Restauration de la configuration du serveur	Non	Non	Non	Non	Non	Non	Oui	Oui
Restauration facile (configuration du système)	Non	Oui	Non	Oui	Non	Oui	Non	Oui
LED/LCD d'intégrité	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Quick Sync (Synchronisation rapide) (lunette NFC nécessaire)	Non	Oui	Non	Oui	Non	S/O	Non	Oui

Tableau 1. Fonctionnalités sous licence dans iDRAC7 et iDRAC8 (suite)

Fonctionnalité	Gestion de base (iDRAC 7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express pour lames	iDRAC8 Express pour lames	iDRAC7 Enterprise	iDRAC8 Enterprise
iDRAC direct (port de gestion USB à l'avant)	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Module des services iDRAC (iSM)	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Collecte SupportAssist (intégré)	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Capture d'écran en cas de panne[5]	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Capture vidéo en cas de panne[5]	Non	Non	Non	Non	Non	Non	Oui	Oui
Capture à l'amorçage	Non	Non	Non	Non	Non	Non	Oui	Oui
Réinitialisation manuelle de l'iDRAC	Non	Oui	Non	Oui	Non	Oui	Non	Oui
NMI virtuel	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Surveillance de l'OS	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Rapport d'intégrité intégré	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Journal des événements système	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Journal Lifecycle	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Notes de travail	Non	Oui	Non	Oui	Non	Oui	Non	Oui
Journal Syslog distant	Non	Non	Non	Non	Non	Non	Oui	Oui
Gestion des licences	Non	Oui	Non	Oui	Non	Oui	Non	Oui

[1] Exige un support de carte média SD.

[2] Les serveurs de série 500, rack inférieur et tour exigent une carte matérielle pour activer cette fonction ; ce matériel est proposé à un coût supplémentaire.

[3] Une fonction de mise à jour sans agent et à distance est disponible uniquement via IPMI.

[4] Disponible uniquement à l'aide d'IPMI.

[5] Nécessite un agent OMSA sur le serveur cible.

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 2. Interfaces et protocoles d'accès à iDRAC

Interface ou protocole	Description
Utilitaire iDRAC Settings (Configuration iDRAC)	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 iDRAC ainsi que d'autres fonctionnalités. Pour accéder à l'utilitaire de configuration iDRAC, appuyez sur `<F2>` au démarrage, puis cliquez sur **iDRAC Settings (Paramètres iDRAC)** sur la page **System Setup Main Menu (Menu principal de configuration système)**.
Interface web d'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 cryptés 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 en 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 droits d'administrateur complets ou être un utilisateur racine 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 micrologiciel est accessible en se connectant à iDRAC via SSH ou telnet. 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 micrologiciel. Une fois que vous êtes entré dans l'invite RACADM, vous pouvez exécuter directement les commandes sans le préfixe racadm.
Panneau LCD du serveur/Panneau LCD du châssis	Utilisez l'écran LCD du panneau avant du serveur pour : ● afficher les alertes, l'adresse IP iDRAC ou l'adresse MAC, des chaînes programmables par l'utilisateur ; ● définir DHCP ; ● configurer les paramètres IP statiques iDRAC. Dans le cas des serveurs lames, l'écran LCD se trouve sur le panneau avant du châssis et il est partagé entre tous les serveurs lames. Pour réinitialiser l'iDRAC sans redémarrer le serveur, appuyez sur le bouton d'identification système durant 16 secondes.
Interface web CMC	Outre la surveillance et la gestion du châssis, utilisez l'interface web CMC pour : ● afficher l'état d'un système géré ; ● mettre à jour le micrologiciel iDRAC ● configurer les paramètres réseau iDRAC ● vous connecter à l'interface web d'iDRAC ● démarrer, arrêter ou réinitialiser le système géré ; ● mettre à jour le BIOS, PERC et les adaptateurs réseau pris en charge.
Lifecycle Controller	Utilisez Lifecycle Controller pour configurer iDRAC. Pour accéder à Lifecycle Controller, appuyez sur <F10> au démarrage et accédez à **System Setup (Configuration du système)** > **Advanced Hardware Configuration (Configuration matérielle avancée)** > **iDRAC Settings (Paramètres iDRAC)**. Pour plus d'informations, consultez le *Guide d'utilisation de Lifecycle Controller* à l'adresse **dell.com/idracmanuals**.
Telnet	Utilisez Telnet pour accéder à iDRAC afin d'exécuter des commandes RACADM et SMCLP. Pour en savoir plus sur RACADM, consultez le *Guide de référence de l'interface en ligne de commande iDRAC RACADM* à l'adresse **dell.com/idracmanuals**. Pour plus d'informations sur l'interface SMCLP, voir Utilisation de SMCLP.

Tableau 2. Interfaces et protocoles d'accès à iDRAC (suite)

Interface ou protocole	Description
	REMARQUE : Telnet n'est pas un protocole sécurisé et il est désactivé par défaut. Telnet transmet toutes les données, y compris les mots de passe en texte clair. Pour transmettre des données sensibles utilisez l'interface SSH
SSH	Utilisez SSH pour exécuter les commandes RACADM et SMCLP. Vous obtenez les mêmes fonctionnalités qu'avec la console Telnet, mais avec une couche de transport cryptée qui renforce la sécurité. Le service SSH est activé par défaut dans iDRAC. Le service SSH peut être désactivé dans iDRAC. iDRAC ne prend en charge que la version 2 de SSH avec l'algorithme de clé d'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 d'utilisation des utilitaires Dell OpenManage Baseboard Management Controller* à l'adresse **dell.com/idracmanuals**. **REMARQUE :** IPMI version 1.5 n'est pas prise en charge.
VMCLI	Utilisez l'interface VMCLI (Virtual Media Command Line Interface) pour accéder à un support distant via la station de gestion et déployer des systèmes d'exploitation sur plusieurs systèmes gérés.
SMCLP	Utilisez Server Management Workgroup Server Management-Command Line Protocol (SMCLP) pour effectuer des tâches de gestion des systèmes. Vous pouvez y accéder via SSH ou Telnet. Pour plus d'informations sur SMCLP, voir Utilisation de SMCLP.
WSMAN	LC-Remote Services repose sur le protocole de gestion WS pour exécuter des tâches de gestion de systèmes un à plusieurs. Vous devez utiliser un client WSMAN, tel que WinRM (Windows) ou le client OpenWSMAN (Linux), pour pouvoir utiliser la fonctionnalité LC-Remote Services. Vous pouvez également utiliser Power Shell et Python pour exécuter des scripts vers l'interface WSMAN. Web Services for Management (WSMAN) est un protocole basé sur Simple Object Access Protocol (SOAP) pour la gestion de systèmes. iDRAC utilise WSMAN pour faire passer les informations de gestion basées sur le modèle Common Information Model (CIM) de l'organisme Distributed Management Task Force (DMTF). Les informations CIM définissent la sémantique et les types d'informations pouvant être modifiés dans un système géré. Les données disponibles via WSMAN sont fournies par l'interface d'instrumentation iDRAC adressée sur les profils DMTF et les profils d'extension. Pour plus d'informations, consultez : • le Lifecycle Controller-Remote Services User's Guide (Guide d'utilisation du Lifecycle Controller-Services à distance) disponible à l'adresse **dell.com/idracmanuals**. • le Lifecycle Controller Integration Best Practices Guide (Guide des meilleures pratiques d'intégration du Lifecycle Controller) disponible à l'adresse **dell.com/support/manuals**. • la page Lifecycle Controller sur le site Dell TechCenter : **delltechcenter.com/page/Lifecycle+Controller** • les scripts WSMAN pour Lifecycle Controller – **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller** • fichiers MOF et profils : **delltechcenter.com/page/DCIM.Library** • Site web DMTF : **dmtf.org/standards/profiles/**

Informations sur les ports iDRAC

Les ports suivants sont requis pour accéder à distance à iDRAC via les 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 ce faire, voir Configuration des services.

Tableau 3. Ports qu'écoute iDRAC pour les connexions

Numéro de port	Type	Fonction	Port configurable	Niveau de cryptage maximum
22	TCP	SSH	Oui	SSL 256 bits
23	TCP	TELNET	Oui	Aucun

Tableau 3. Ports qu'écoute iDRAC pour les connexions (suite)

Numéro de port	Type	Fonction	Port configurable	Niveau de cryptage maximum
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
5900	TCP	Redirection du clavier et de la souris de la console, média virtuel, dossiers virtuels et partage de fichier distant	Oui	SSL 128 bits
5901	TCP	VNC	Oui	SSL 128 bits
REMARQUE : Port 5901 ouvert lorsque la fonctionnalité VNC est activée.				

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

Tableau 4. Ports qu'iDRAC utilise comme client

Numéro de port	Type	Fonction	Port configurable	Niveau de cryptage maximum
25	TCP	SMTP	Oui	Aucun
53	UDP	DNS	Non	Aucun
68	UDP	Adresse IP attribuée par DHCP	Non	Aucun
69	TFTP	TFTP	Non	Aucun
123	UDP	Protocole de temps de réseau (NTP)	Non	Aucun
162	UDP	Interruption SNMP	Oui	Aucun
445	TCP	CIFS (Common Internet File System)	Non	Aucun
636	TCP	LDAPS (LDAP Over SSL)	Non	SSL 256 bits
2049	TCP	NFS (Network File System)	Non	Aucun
3 269	TCP	LDAPS pour le catalogue global (CG)	Non	SSL 256 bits
5353	UDP	mDNS	Non	Aucun
514	UDP	Syslog distant	Oui	Aucun

Autres documents utiles

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

- L'*Aide en ligne iDRAC* fournit des informations détaillées sur les champs disponibles dans l'interface Web iDRAC, ainsi que leur description. Vous pouvez y accéder après avoir installé iDRAC.
- Le *Guide de référence de l'interface de ligne de commande RACADM iDRAC* fournit des informations sur les sous-commandes RACADM, les interfaces prises en charge, les groupes de bases de données des propriétés iDRAC et les définitions d'objets.
- La *iDRAC RACADM Support Matrix* (Matrice de prise en charge RACADM iDRAC) fournit la liste des sous-commandes et objets qui sont applicables à une version d'iDRAC spécifique.
- Le *Guide de présentation de Systems Management* fournit des informations sur les logiciels disponibles pour exécuter des tâches de gestion de systèmes.
- Le *Guide d'utilisation de l'interface utilisateur graphique du Dell Lifecycle Controller* pour serveurs Dell PowerEdge de 12e génération et 13e génération fournit des informations sur l'utilisation de l'interface utilisateur graphique (GUI) de Lifecycle Controller.
- Le *Dell Lifecycle Controller Remote Services For 13th Generation Dell PowerEdge Servers Quick Start Guide* (Guide de démarrage rapide des services distants Dell Lifecycle Controller pour les serveurs Dell PowerEdge de 13e génération) présente les capacités des

services distants, fournit des informations sur la mise en route des services distants et de l'interface API du Lifecycle Controller et fournit des références pour les différentes ressources du centre Dell TechCenter.

- Le *Dell Remote Access Configuration Tool User's Guide* (Guide d'utilisation de l'outil de configuration de l'accès à distance Dell) explique comment utiliser l'outil de détection des adresses IP iDRAC dans le réseau et comment exécuter des mises à jour de micrologiciel un à plusieurs et des configurations Active Directory pour les adresses IP découvertes.
- Le document *Matrice de prise en charge logicielle des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- L'*iDRAC Service Module User's Guide* (Guide d'utilisation du module Service iDRAC) fournit des informations sur l'installation du module Service iDRAC.
- Le *Guide d'installation de Dell OpenManage Server Administrator* contient les instructions d'installation de Dell OpenManage Server Administrator.
- Le *Guide d'installation de Dell OpenManage Management Station Software* contient les instructions d'installation du logiciel de station de gestion Dell OpenManage qui inclut l'utilitaire de gestion de la carte mère, les outils DRAC et le snap-in d'Active Directory.
- Le *Guide d'utilisation des utilitaires de gestion des contrôleurs Dell OpenManage Baseboard Management* contient des informations sur l'interface IPMI.
- Les *Notes de mise à jour* fournissent des mises à jour de dernière minute du système ou de la documentation ou encore des informations techniques avancées destinées aux utilisateurs expérimentés ou aux techniciens.
- Le *Glossaire* fournit des informations sur les termes utilisés dans ce document.

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

- Le document « Safety instructions » (Consignes de sécurité) fourni avec votre système contient des informations importantes sur la sécurité et les réglementations en vigueur. Pour plus d'informations réglementaires, voir la page d'accueil Regulatory Compliance 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 les fonctionnalités du système, les procédures de configuration et les caractéristiques techniques.
- Le *Manuel du propriétaire* fournit des informations concernant les fonctionnalités du système et explique comment dépanner le système et installer ou remplacer des composants système.

Tâches associées

Contacter Dell , page 28
Accès aux documents à partir du site de support Dell EMC , page 29

Référence des médias sociaux

Pour en savoir plus sur le produit, les pratiques d'excellence et les informations concernant les services et solutions Dell, vous pouvez accéder aux plateformes des réseaux sociaux comme Dell TechCenter. Vous pouvez accéder aux blogs, forums, livres blancs, vidéos de démonstration, etc. sur la page wiki iDRAC à l'adresse **www.delltechcenter.com/idrac**.

Pour consulter des documents concernant iDRAC ou les autres micrologiciels associés, reportez-vous à **dell.com/idracmanuals** et à **dell.com/esmmanuals**.

Contacter Dell

REMARQUE : Si vous ne possédez pas une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, acte de vente ou catalogue de produits Dell.

Dell offre plusieurs options de service et de support en ligne et par téléphone. La disponibilité des produits varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre région. Pour contacter le service commercial, technique ou client de Dell :

1. Rendez-vous sur **Dell.com/support**.
2. Sélectionnez la catégorie d'assistance.
3. Rechercher votre pays ou région dans le menu déroulant **Choisissez un pays ou une région** situé au bas de la page.
4. Sélectionnez le lien de service ou de support en fonction de vos besoins.

Accès aux documents à partir du site de support Dell EMC

Vous pouvez accéder aux documents requis en utilisant l'un des liens suivants :

- Pour les documents de gestion des systèmes Dell EMC Enterprise : **www.dell.com/SoftwareSecurityManuals**
- Pour les documents Dell EMC OpenManage : **www.dell.com/OpenManageManuals**
- Pour les documents de gestion des systèmes Dell EMC Enterprise à distance : **www.dell.com/esmmanuals**
- Pour les documents iDRAC et Dell EMC Lifecycle Controller : **www.dell.com/idracmanuals**
- Pour les documents de gestion des systèmes Dell EMC Enterprise - Connexions OpenManage : **www.dell.com/OMConnectionsEnterpriseSystemsManagement**
- Pour les documents Dell EMC Outils de facilité de la gestion : **www.dell.com/ServiceabilityTools**
- 1. Rendez-vous sur **www.support.Dell.com**.
  2. Cliquez sur **Parcourir tous les produits**.
  3. Sur la page **Tous les produits**, cliquez sur **Logiciel** et cliquez sur le lien requis parmi les suivants :
     - **Analyses**
     - **Gestion des systèmes Client**
     - **Applications d'entreprise**
     - **Gestion des systèmes Enterprise**
     - **Solutions du secteur public**
     - **Utilitaires**
     - **Mainframe**
     - **Outils de facilité de la gestion**
     - **Solutions de virtualisation**
     - **Systèmes d'exploitation**
     - **Compatibilité**
  4. Pour afficher un document, cliquez sur le produit requis, puis sur la version requise.
- Avec les moteurs de recherche :
  - Saisissez le nom et la version du document dans la zone de recherche.

2

Ouverture de session dans iDRAC

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

REMARQUE :

- Vous devez disposer du privilège de connexion à iDRAC pour pouvoir ouvrir une session dans iDRAC.
- L'interface utilisateur graphique de l'iDRAC ne prend pas en charge les boutons de navigateur comme **Reculer**, **Avancer** ou **Actualiser**.

REMARQUE : Pour plus d'informations sur les caractères recommandé pour les noms d'utilisateur et les mots de passe, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

Tâches associées

Ouverture de session dans iDRAC en tant qu'utilisateur local, utilisateur Active Directory ou utilisateur LDAP , page 30
Connexion au contrôleur CMC avec une carte à puce , page 31
Ouverture d'une session iDRAC à l'aide de la connexion directe , page 33
Modification du mot de passe d'ouverture de session par défaut , page 35

Sujets :

- Ouverture de session dans iDRAC en tant qu'utilisateur local, utilisateur Active Directory ou utilisateur LDAP
- Connexion au contrôleur CMC avec une carte à puce
- Ouverture d'une session iDRAC à l'aide de la connexion directe
- Accès à l'iDRAC à l'aide de l'interface distante RACADM
- Accès à l'iDRAC à l'aide de l'interface locale RACADM
- Accès à l'iDRAC à l'aide de RACADM du micrologiciel
- Accès à l'iDRAC à l'aide de SMCLP
- Connexion à l'iDRAC à l'aide de l'authentification par clé publique
- Sessions iDRAC multiples
- Modification du mot de passe d'ouverture de session par défaut
- Activation ou désactivation du message d'avertissement du mot de passe par défaut
- Blocage d'adresse IP
- informations d'identification des mots de passe non valides

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.

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

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

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

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**, tapez `https://[iDRAC-IP-address]` et appuyez sur <Entrée>.

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

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

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

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

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

Concepts associés

Configuration des comptes et des privilèges des utilisateurs , page 133
Modification du mot de passe d'ouverture de session par défaut , page 35

Tâches associées

Configuration des navigateurs web pris en charge , page 59

Connexion au contrôleur CMC avec une carte à puce

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

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

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

Tâches associées

Ouverture de session dans l'iDRAC en tant qu'utilisateur local à l'aide d'une carte à puce , page 31
Ouverture de session dans l'iDRAC comme utilisateur Active Directory par carte à puce , page 32

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 :

- Téléversez le certificat d'utilisateur de carte à puce et le certificat d'autorité de certification (CA) de confiance vers 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.

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

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

1. Accédez à l'interface Web d'iDRAC en utilisant 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 (443) a été changé, tapez `https://[IP address]:[port number]` , où `[IP address]` est l'adresse IP d'iDRAC et `[port number]` est le numéro de port HTTPS.

2. Insérez la carte à puce dans le lecteur et cliquez sur **Ouvrir une session**.
   Une invite demande le code PIN de la carte. Aucun mot de passe n'est nécessaire.
3. Entrez le code PIN de la carte pour les utilisateurs de carte à puce locaux.

   Vous avez ouvert une session sur l'iDRAC.

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

Concepts associés

Activation ou désactivation de l'ouverture de session par carte à puce , page 159

Tâches associées

Configuration d'ouverture de session iDRAC par carte à puce pour les utilisateurs locaux , page 158

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

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

- Téléversez un certificat d'autorité de certification (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 iDRAC en utilisant 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 (443) est modifié, tapez `https://[IP address]:[port number]`, où `[IP address]` est l'adresse IP iDRAC et `[port number]` est le numéro de port HTTPS.

2. Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.
   La fenêtre contextuelle du **code PIN** s'affiche.
3. Saisissez le code 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.

Concepts associés

Activation ou désactivation de l'ouverture de session par carte à puce , page 159

Tâches associées

Configuration de la connexion par carte à puce iDRAC pour les utilisateurs Active Directory , page 159

Ouverture d'une session iDRAC à l'aide de la connexion directe

Lorsque la connexion directe (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.

Concepts associés

Configuration d'ouverture de session par connexion directe (SSO) iDRAC pour les utilisateurs Active Directory , page 157

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 par connexion directe (SSO), vérifiez que :

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

Pour ouvrir une session dans 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, tapez `https://[FQDN address]`

   REMARQUE : Si le numéro de port HTTPS par défaut (443) a été changé, tapez `https://[FQDN address]:[port number]`, où `[FQDN address]` est le nom de domaine complet qualifié iDRAC (nomdnsiDRAC.nom.domaine) et `[port number]` est le numéro de port HTTPS.

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

   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.

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

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

Si le LAN réseau iDRAC est désactivé (LAN activé = non), SSO n'est pas disponible.

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

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

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

Vous pouvez utiliser l'interface distante RACADM pour accéder à l'iDRAC à l'aide de l'utilitaire RACADM.

Pour en savoir plus, voir l'*iDRAC RACADM Command Line Interface Reference Guide* (Guide de référence de l'interface de ligne de commande RACADM iDRAC) disponible à l'adresse **dell.com/idracmanuals**.

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

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

Tâches associées

Validation d'un certificat d'autorité de certification (CA) pour utiliser l'interface distante RACADM sur Linux , page 34

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 du module de certificat d'autorité de certification par défaut sur la station de gestion. Par exemple, pour RHEL5 64 bits, il s'agit de **/etc/pki/tls/cert.pem**.
3. Ajoutez le certificat PEM d'autorité de certification au certificat d'autorité de certification de la station de gestion.

   Par exemple, utilisez la `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

Pour plus d'informations sur l'accès à l'iDRAC à l'aide de l'interface RACADM locale, voir l'*iDRAC RACADM Command Line Interface Reference Guide* (Guide de référence de l'interface de ligne de commande RACADM iDRAC), disponible à l'adresse **dell.com/idracmanuals**.

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

Vous pouvez utiliser l'interface SSH ou Telnet pour accéder à l'iDRAC et exécuter des commandes RACADM du micrologiciel. Pour en savoir plus, voir l'*iDRAC RACADM Command Line Interface Reference Guide* (Guide de référence de l'interface de ligne de commande RACADM iDRAC) disponible à l'adresse **dell.com/idracmanuals**.

Accès à l'iDRAC à l'aide de SMCLP

SMCLP est l'invite de ligne de commande par défaut lorsque vous ouvrez une session dans l'iDRAC à l'aide de Telnet ou SSH. Pour en savoir plus, voir Utilisation de SMCLP.

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

Vous pouvez vous connecter à l'iDRAC sur SSH sans entrer de mot de passe. Vous pouvez également envoyer une simple commande RACADM comme argument de ligne de commande à l'application SSH. Les options de ligne de commande fonctionnent pratiquement comme l'interface distante RACADM 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 d'iDRAC.

Envoi de commandes RACADM :

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

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

Concepts associés

Utilisation de l'authentification par clé publique pour SSH , page 129

Sessions iDRAC multiples

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

Tableau 5. Sessions iDRAC multiples

Interface	Nombre de sessions
Interface web iDRAC	6
Interface RACADM distante	4
Micrologiciel RACADM/SMCLP	SSH - 2 Telnet - 2 Série - 1

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

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

- Vous vous connectez à iDRAC avec le privilège de Configuration.
- La fonction d'avertissement de mot de passe par défaut est activée.
- Les coordonnées de tout compte actuellement activé sont root/calvin.
- L'option Forcer la modification du mot de passe (FCP) est activée.

REMARQUE : Lorsque l'attribut FCP est activé, vous devez modifier le mot de passe par défaut. Vous serez ensuite authentifié et autorisé à accéder à l'iDRAC de manière habituelle.

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

REMARQUE : Pour plus d'informations sur les caractères recommandés pour les noms d'utilisateur et les mots de passe, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

Tâches associées

Activation ou désactivation du message d'avertissement du mot de passe par défaut , page 36

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

Lorsque vous ouvrez une session sur l'interface web d'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 :

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

   REMARQUE : Pour plus d'informations sur les caractères recommandé pour les noms d'utilisateur et les mots de passe, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

3. Dans le champ **Confirmer le mot de passe**, saisissez de nouveau le mot de passe.
4. Cliquez sur **Continuer**. Le nouveau mot de passe est configuré et votre session s'ouvre sur l'iDRAC.

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

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

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

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

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

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

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

REMARQUE : Pour plus d'informations sur les caractères recommandé pour les noms d'utilisateur et les mots de passe, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

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

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

1. Dans l'utilitaire de configuration iDRAC, accédez à **Configuration de l'utilisateur**.
   La page **Paramètres iDRAC - Configuration de l'utilisateur** s'affiche.
2. Dans le champ **Modifier le mot de passe**, saisissez le nouveau mot de passe.

   REMARQUE : Pour plus d'informations sur les caractères recommandé pour les noms d'utilisateur et les mots de passe, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les informations sont enregistrées.

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

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

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

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

1. Allez sous **Présentation** > **Paramètres iDRAC** > **Authentification utilisateur** > **Utilisateurs locaux**.
   La page **Utilisateurs** s'affiche.
2. Dans la section **Avertissement de mot de passe par défaut**, sélectionnez **Activer**, puis cliquez sur **Appliquer** pour activer l'affichage de la page **Avertissement de mot de passe par défaut** lorsque vous ouvrez une sessions sur iDRAC. Sinon, sélectionnez **Désactiver**.

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

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

Pour activer l'affichage du message d'avertissement de modifier le mot de passe d'ouverture de session par défaut à l'aide de RACADM, utilisez l'objet `idrac.tuning.DefaultCredentialWarning`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Blocage d'adresse IP

Le blocage d'adresse IP détermine de manière dynamique un nombre consécutif d'échecs de connexion issus d'une adresse IP particulière et empêche cette adresse de se connecter à l'iDRAC durant une période prédéfinie (l'adresse est bloquée). Le blocage d'adresse IP inclut :

- le nombre d'échecs de connexion autorisé ;
- le délai (en secondes) pendant lequel ces échecs doivent avoir lieu ;
- le délai en secondes pendant lequel l'adresse IP bloquée ne peut pas établir de session lorsque le nombre d'échecs autorisé est atteint.

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

REMARQUE : Quand plusieurs tentatives de connexion consécutives sont refusées pour une adresse IP, certains clients SSH peuvent afficher ce message :

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

.

Tableau 6. Propriétés de restriction des nouvelles tentatives de connexion

Propriété	Définition
`iDRAC.IPBlocking.BlockEnable`	Active la fonctionnalité de blocage des adresses IP. En cas d'échecs consécutifs (`iDRAC.IPBlocking.FailCount`) pour une même adresse IP dans un certain laps de temps (`iDRAC.IPBlocking.FailWindow`

Tableau 6. Propriétés de restriction des nouvelles tentatives de connexion (suite)

Propriété	Définition
	), les tentatives ultérieures d'établissement de session pour cette adresse sont refusées pendant une certaine durée (`iDRAC.IPBlocking.PenaltyTime`).
`iDRAC.IPBlocking.FailCount`	Définit le nombre d'échecs d'ouverture de session depuis une adresse IP après lequel les nouvelles tentatives de connexion sont refusées.
`iDRAC.IPBlocking.FailWindow`	Le délai en secondes pendant lequel les échecs de connexion sont comptabilisés. Quand le nombre d'échecs atteint cette limite, le compteur s'arrête.
`iDRAC.IPBlocking.PenaltyTime`	La durée en secondes pendant laquelle les tentatives d'ouverture de session depuis une adresse IP sont rejetées après un trop grand nombre d'échecs.

informations d'identification des mots de passe non valides

Pour offrir une sécurité contre les utilisateurs non autorisés et les attaques par déni de service (DoS), l'iDRAC fournit les informations suivantes avant de bloquer l'IP et les interruptions SNMP (si activé) :

- Série d'erreurs de connexion et alertes
- Augmentation des intervalles de temps à chaque tentative séquentielle de connexion incorrecte
- Entrées de journal

REMARQUE : Il est possible de consulter les erreurs et alertes de connexion, les augmentations des intervalles à chaque connexion incorrecte et les entrées de journal à l'aide de n'importe laquelle des interfaces iDRAC, notamment l'interface web, Telnet, SSH, RACADM à distance, WSMAN et VMCLI.

Tableau 7. Comportement de l'interface web iDRAC avec des tentatives de connexion incorrectes

Tentatives de connexion	Blocage (secondes)	Erreur consignée (USR00034)	Message d'affichage GUI	Alerte SNMP (si cette fonction est activée)
Première connexion incorrecte	0	Non	Aucun	Non
Deuxième connexion incorrecte	0	Non	Aucun	Non
Troisième connexion incorrecte	600	Oui	• `RAC0212 : Login failed. Verify that username and password is correct. Login delayed for 600 seconds.` • Le bouton **Try again** (Réessayer) est désactivé pendant 600 secondes.	Oui

REMARQUE : Par défaut, le compteur d'échecs est remis à zéro après 600 secondes. Toutefois, vous pouvez le personnaliser en modifiant le délai PenaltyTime via l'interface RACADM. Utilisez la commande *setidrac.ipblockingpenaltyTime X*.

3

Installation du système géré et de la station de gestion

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

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

iDRAC Express et iDRAC Enterprise sont livrés par l'usine dotés d'une adresse IP statique par défaut. Cependant, Dell offre également deux options :

- **Serveur de provisionnement** : utilisez cette option si un serveur de provisionnement est installé dans l'environnement de votre centre de données. Un serveur de provisionnement gère et automatise le déploiement ou la mise à niveau d'un système d'exploitation et d'une application pour un serveur Dell PowerEdge. Si vous activez l'option Serveur de provisionnement, les serveurs, lors du premier démarrage, recherchent un serveur de provisionnement afin d'en prendre le contrôle et de commencer le déploiement automatisé ou le processus de mise à niveau.
- **DHCP** : utilisez cette option si un serveur DHCP (Dynamic Host Configuration Protocol, Protocole de configuration dynamique d'hôte) est installé dans l'environnement de votre centre de données ou si vous utilisez la Configuration automatique d'iDRAC ou le Gestionnaire de configuration d'OpenManage Essentials pour automatiser le provisionnement du serveur. Le serveur DHCP attribue automatiquement l'adresse IP, la passerelle et le masque de sous-réseau de l'iDRAC.

Vous pouvez activer la découverte automatique ou le protocole DHCP lors de la commande du serveur. Aucun frais n'est lié à l'activation de ces fonctionnalités. Toutefois, une seule configuration est possible.

Concepts associés

Définition de l'adresse IP d'iDRAC , page 39
Installation du système géré , page 51
Mise à jour du micrologiciel de périphérique , page 64
Restauration du micrologiciel du périphérique , page 73

Tâches associées

Installation de la station de gestion , page 51
Configuration des navigateurs web pris en charge , page 59

Sujets :

- Définition de l'adresse IP d'iDRAC
- Installation de la station de gestion
- Installation du système géré
- Configuration des navigateurs web pris en charge
- Mise à jour du micrologiciel de périphérique
- Affichage et gestion des mises à jour planifiées
- Restauration du micrologiciel du périphérique
- Sauvegarde du profil du serveur
- Importation du profil du serveur
- Surveillance d'iDRAC à l'aide d'autres outils de gestion de systèmes

Définition de l'adresse IP d'iDRAC

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

- Utilitaire de configuration iDRAC

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

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

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

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

Après avoir défini l'adresse IP d'iDRAC :

- Veillez à changer le nom d'utilisateur et le mot de passe par défaut après avoir configuré l'adresse IP d'iDRAC.
- 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) : exige un client, tel que PuTTY sur Windows. SSH est disponible par défaut dans la plupart des systèmes Linux et il ne nécessite donc pas de client.
  - Telnet (doit être activé, car il est désactivé par défaut)
  - IPMITool (utilise la commande IPMI) ou l'invite de shell (nécessite le programme d'installation personnalisé Dell dans Windows ou Linux, disponible depuis le DVD *Systems Management Documentation and Tools* ou sur le site **dell.com/support**)

Tâches associées

Définition de l'adresse IP d'iDRAC à l'aide de l'utilitaire de configuration d'iDRAC , page 40
Définition de l'adresse IP d'iDRAC à l'aide de l'interface Web CMC , page 43
Activation du serveur de provisionnement , page 44
Configuration des serveurs et des composants du serveur à l'aide de la Configuration automatique , page 44

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 <F2> pendant l'auto-test de démarrage (POST).
3. Sur la page **System Setup Main Menu**, cliquez sur **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.

Tâches associées

Paramètres réseau , page 41
Paramètres communs , page 42
Paramètres IPv4 , page 42
Paramètres IPv6 , page 42
Paramètres IPMI , page 43
Paramètres VLAN , page 43

Paramètres réseau

Pour configurer les paramètres réseau :

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

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

     Cette option implique que le port réseau dédié d'iDRAC achemine son trafic séparément des ports LOM ou NIC du serveur. En ce qui concerne la gestion du trafic, 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.

     REMARQUE : Dans le cas de serveurs lames, l'option Dédié s'affiche sous la forme de **Châssis (dédié)**.
   - **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. Dans les serveurs lames avec deux ports NDC, deux options LOM (LOM1 et LOM2) sont disponibles et sur les serveurs à quatre ports NDC, les quatre options LOM sont disponibles.

   REMARQUE : L'option LOM partagé n'est pas prise en charge sur les cartes bNDC suivantes si elles sont utilisées dans un serveur pleine hauteur - avec deux cartes fille réseau (NDC) parce qu'elles ne prennent pas en charge l'arbitrage de matériel :
   - bNDC Intel 2P X520-k 2P 10 G
   - bNDC Emulex OCM14102-N6-D 10 Gbits
   - bNDC Emulex OCm14102-U4-D 10 Gbits
   - bNDC Emulex OCm14102-U2-D 10 Gbits
   - bNDC QLogic QMD8262-k DP 10 G

3. Dans le menu déroulant **Failover Network (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 : Si vous avez sélectionné, **Dédié** dans le menu déroulant **Sélection NIC**, l'option est grisée.

   REMARQUE : Le basculement est pas pris en charge sur le LOM partagé pour les rNDC et bNDC Emulex :
   - rNDC Emulex OCM14104-UX-D 10 Gbitsx
   - rNDC Emulex OCM14104-U1-D 10 Gbits
   - rNDC Emulex OCM14104B-U1-D 10 Gbits
   - rNDC Emulex OCM14104-N1-D 10 Gbits
   - rNDC Emulex OCM14104B-N1-D 10 Gbits
   - bNDC Emulex OCM14102-U2-D 10 Gbits
   - bNDC Emulex OCM14102-U4-D 10 Gbits
   - bNDC Emulex OCM14102-N6-D 10 Gbits

   REMARQUE : Sur les serveurs Dell PowerEdge FM120x4 et FX2, **Réseau de basculement** n'est pas pris en charge pour les configurations de traîneau de châssis. Pour en savoir plus sur les configurations des traîneaux de châssis, voir le Guide d'utilisation du contrôleur CMC (Chassis Management Controller) disponible sur **dell.com/idracmanuals**.

   REMARQUE : Sur les serveurs PowerEdge FM120x4, lors de la configuration de l'isolation de l'adaptateur réseau amélioré, assurez-vous que le LOM2 est désactivé sur le système hôte et qu'il n'est pas sélectionné pour la carte réseau iDRAC. Pour en

savoir plus sur les configurations des traîneaux de châssis, voir le Guide d'utilisation du contrôleur CMC (Chassis Management Controller) disponible sur **dell.com/idracmanuals**.

4. 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.
5. 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.

6. Sous **Mode duplex**, sélectionnez l'option **Semi duplex** ou **Duplex intégral**.

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

Paramètres communs

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

Pour enregistrer iDRAC :

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

Paramètres IPv4

Pour configurer les paramètres IPv4 :

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

Paramètres IPv6

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

Pour configurer les paramètres iPv6 :

1. Sélectionnez l'option **Activé** sous **Activer IPv6**.
2. Pour que le serveur DHCPv6 affecte automatiquement l'adresse IP, la passerelle et le masque de sous-réseau à iDRAC, sélectionnez l'option **Activé** sous **Activer la configuration automatique**.

   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 0 et128.
5. Dans la zone **Passerelle statique**, entrez l'adresse de la passerelle.

   REMARQUE : Si vous configurer 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.

6. Si vous utilisez DHCP, activez **DHCPv6 pour obtenir les adresses des serveurs DNS** pour obtenir les adresses des serveurs DNS principal et secondaire du serveur DHCPv6. Vous pouvez configurer les éléments suivants au besoin :
   - Dans la zone **Serveur DNS statique préféré**, entrez l'adresse IPv6 statique du serveur DNS.
   - Dans la zone **Serveur DNS statique secondaire**, entrez le serveur DNS secondaire statique.

Paramètres IPMI

Pour activer les paramètres IPMI :

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

Paramètres VLAN

Vous pouvez configurer l'iDRAC dans l'infrastructure VLAN. Pour configurer les paramètres VLAN, procédez comme suit :

REMARQUE : Sur les serveurs lames qui sont configurés sur **Chassis (Dédié)**, les paramètres VLAN sont en lecture seule et ne peuvent être modifiées qu'à l'aide du CMC. Si le serveur est configuré en mode partagé, vous pouvez configurer les paramètres VLAN en mode partagé dans l'iDRAC.

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.

Définition de l'adresse IP d'iDRAC à l'aide de l'interface Web CMC

Pour définir l'adresse IP d'iDRAC à l'aide de l'interface Web :

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

1. Ouvrez une session dans l'interface Web CMC.
2. Accédez à **Server Overview** > **Setup** > **iDRAC** (Présentation du serveur, Configurer, iDRAC).
   La page **Déployer iDRAC** s'affiche.
3. Sous **Paramètres réseau iDRAC**, sélectionnez **Activer LAN** et les autres paramètres réseau en fonction des besoins. Pour plus d'informations, voir l'*aide en ligne de CMC*.
4. Pour d'autres paramètres réseau spécifiques de chaque serveur lame, accédez à **Présentation du serveur** > **<nom serveur>**.
   La page **Condition du serveur** s'affiche.
5. Cliquez sur **Lancer iDRAC** et accédez à **Présentation** > **Paramètres iDRAC** > **Réseau**.
6. Dans la page **Réseau**, définissez les paramètres réseau suivants :
   - Paramètres réseau
   - Paramètres communs
   - Paramètres IPv4
   - Paramètres IPv6
   - Paramètres IPMI
   - Paramètres VLAN

   REMARQUE : Pour en savoir plus, voir l'*Aide en ligne d'iDRAC*.

7. Pour enregistrer les informations réseau, cliquez sur **Appliquer**.

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

Activation du serveur de provisionnement

La fonction de Serveur de provisionnement permet aux serveurs nouvellement installés de découvrir automatiquement la console de gestion à distance qui héberge le serveur de provisionnement. Le *serveur de provisionnement* fournit des références d'utilisateur administratif personnalisées à l'iDRAC afin de faciliter la découverte et la gestion du serveur non provisionné depuis la console de gestion. Pour en savoir plus sur le serveur de provisionnement, voir le *Lifecycle Controller Remote Services User's Guide* (Guide d'utilisation des services à distance Lifecycle Controller) disponible à l'adresse **dell.com/idracmanuals**.

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

Vous pouvez activer la fonction de Serveur de provisionnement à l'aide de l'utilitaire de Paramètres d'iDRAC ou du Lifecycle Controller. Pour plus d'informations sur l'utilisation du Lifecycle Controller, voir le *Lifecycle Controller User's Guide* (Guide d'utilisation du Lifecycle Controller) disponible à l'adresse **dell.com/idracmanuals**.

Si le serveur de provisionnement n'est pas activé sur le système livré par l'usine, le compte d'administrateur par défaut (nom d'utilisateur : root et mot de passe : calvin) est activé. Avant d'activer le serveur de provisionnement, veillez à désactiver le compte d'administrateur. Si la fonction de serveur de provisionnement du Lifecycle Controller est activée, tous les comptes d'utilisateur iDRAC sont désactivés tant que le serveur de provisionnement n'est pas *découvert*.

Pour activer le serveur de provisionnement, utilisez l'utilitaire de Paramètres d'iDRAC :

1. Mettez le système sous tension.
2. Au cours du 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 découverte automatique, entrez l'adresse IP du serveur d'approvisionnement et cliquez sur **Retour**.

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

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

   REMARQUE : IPv6 n'est pas pris en charge pour la découverte automatique.

7. Activez DHCP et obtenez le nom de domaine, l'adresse du serveur DNS et le nom de domaine DNS depuis DHCP.

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

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

La fonction 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 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 CIFS ou NFS qui est accessible par le serveur DHCP et iDRAC du serveur en cours de configuration. Le nom du fichier SCP peut être basé sur le numéro 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, son emplacement, ainsi que les références utilisateur permettant d'accéder à l'emplacement du fichier.

REMARQUE : CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.

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.

REMARQUE :

- Vous pouvez activer la configuration automatique uniquement si 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. Pour plus d'informations sur l'activation de la configuration automatique, voir Activation de la configuration automatique à l'aide de RACADM , page 49.

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 requis. `Config.xml` est la valeur par défaut du nom du fichier SCP.

Vous pouvez 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. Par exemple, s'il existe deux modèles de serveur à configurer, PowerEdge R730s et PowerEdge R530s, utilisez deux fichiers SCP, `R730-config.xml` et `R530-config.xml`.

REMARQUE : Sur les systèmes dotés de l'iDRAC version 2.20.20.20 et versions ultérieures, si le paramètre de nom de fichier est absent de l'option DHCP 60, l'agent de configuration du serveur iDRAC génère automatiquement le nom de fichier de configuration à l'aide du numéro de service du serveur, du numéro de modèle ou du nom de fichier par défaut, `config.xml`.

L'agent de configuration de serveur iDRAC utilise les règles dans l'ordre suivant pour déterminer quel fichier SCP du partage de fichiers appliquer pour chaque iDRAC :

1. Le nom de fichier spécifié dans l'option DHCP 60.
2. `<ServiceTag>-config.xml` : si un nom de fichier n'est pas spécifié dans l'option DHCP 60, utilisez le numéro de service du système pour identifier de manière unique le fichier SCP correspondant au système. Par exemple, `CDVH7R1-config.xml`
3. `<Model number>-config.xml` : si le nom de fichier de l'option 60 n'est pas spécifié et que le fichier `<Service Tag>-config.xml` est introuvable, utilisez le numéro de modèle du système comme base du nom du fichier SCP à utiliser. Par exemple, `R520-config.xml`.
4. `config.xml` : si les fichiers basés sur le nom de fichier de l'option 60, sur le numéro de service et sur le numéro de modèle ne sont pas disponibles, utilisez le fichier par défaut `config.xml`.

REMARQUE : Pour définir le profil de charge de traitement, ainsi que d'autres attributs à l'aide de SCP, assurez-vous d'exécuter la tâche d'importation SCP deux fois pour obtenir les modifications de configuration correctes.

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.

Pour le firmware iDRAC 2.70.70.70 et versions ultérieures, 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 :

- « <numéro de série>-config.xml » (exemple : CDVH7R1-config.xml)
- « <numéro de modèle>-config.xml » (exemple : R630-config.xml)
- « config.xml »
- « <numéro de série>-config.json » (exemple : CDVH7R1-config.json)
- « <numéro de modèle>-config.json » (exemple : R630-config.json)
- « config.json »

Concepts associés

Séquence de configuration automatique , page 45
Options DHCP , page 46

Tâches associées

Activation de la configuration automatique à l'aide de l'interface Web de l'iDRAC , page 49
Activation de la configuration automatique à l'aide de RACADM , page 49

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. L'iDRAC dans le cadre de l'acquisition de l'adresse IP annonce l'iDRAC identifiant de classe fournisseur. (Option 60)
5. Le serveur DHCP fait correspondre la classe de fournisseur à l'option de fournisseur dans le fichier `dhcpd.conf` et envoie l'emplacement du fichier 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 la transmission, aux clients DHCP, d'un grand nombre de paramètres définis globalement. Chaque paramètre est reconnu comme une option DHCP. Chaque option est identifiée par un numéro d'option, qui a une valeur de 1 octet. Les numéros d'option 0 et 255 sont réservés au remplissage et aux options de fin, respectivement. Toutes les autres valeurs sont disponibles pour la définition des options.

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

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

Tâches associées

Configuration de l'option 43 sur Windows , page 46
Configuration de l'option 60 sur Windows , page 46
Configuration de l'option 43 et de l'option 60 sur Linux , page 48

Configuration de l'option 43 sur Windows

Pour configurer l'option 43 sur Windows :

1. Sur le serveur DHCP, allez dans **Démarrer** > **Outils d'administration** > **DHCP** pour ouvrir l'outil d'administration de serveur DHCP.
2. Trouvez le serveur et développez tous les éléments de la section.
3. Effectuez un clic droit sur **Options d'étendue** et sélectionnez **Configurer les options**.
   La boîte de dialogue **Options d'étendue** s'affiche.
4. Faites défiler la fenêtre et sélectionnez **043 Informations spécifiques sur le fournisseur**.
5. Dans le champ **Entrée de données**, cliquez n'importe où dans la zone située sous **ASCII** et entrez l'adresse IP du serveur sur lequel se situe l'emplacement de partage, qui contient le fichier de configuration XML.
   La valeur s'affiche lorsque vous la tapez sous l'**ASCII**, mais elle apparaît également en binaire sur la gauche.
6. Cliquez sur **OK** pour enregistrer la configuration.

Configuration de l'option 60 sur Windows

Pour configurer l'option 60 sur Windows :

1. Sur le serveur DHCP, 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**, entrez 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 le menu déroulant, sélectionnez **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 :
    - Fichier (-f) : indique le nom du fichier XML Server Configuration Profile exporté. L'indication de ce nom de fichier est optionnelle avec l'iDRAC versions 2.20.20.20 et ultérieures.

      REMARQUE : Pour plus d'informations sur les règles d'attribution de nom aux fichiers, voir 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 Indique NFS et 2 indique CIFS.

      REMARQUE : 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 d'option -s 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.
    - 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.
    - 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.
    - ProxyDefault (-pd) : indique d'utiliser le paramètre de proxy par défaut (en option).
    - ProxyType (-pt) : saisissez http ou socks (paramètre par défaut : http) (en option).
    - ProxyHost (-ph) : adresse IP de l'hôte proxy (en option).
    - ProxyUserName (-pu) : indique le nom d'utilisateur ayant accès au serveur proxy (obligatoire pour la prise en charge du proxy).
    - ProxyPassword (-pp) : indique le mot de passe de l'utilisateur qui a accès au serveur proxy (obligatoire pour la prise en charge du proxy).

- ProxyPort (-po) : port du serveur proxy (paramètre par défaut : 80) (en option).
- Timeout (to) : indique le délai d'expiration de la nouvelle tentative en minutes pour obtenir le fichier de profil (paramètre par défaut = 60)

REMARQUE : Sur les serveurs DHCP exécutant le système d'exploitation Windows avec une version d'iDRAC antérieure à 2.20.20.20, assurez-vous d'ajouter un espace avant le (-f).

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

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 XML Server Configuration Profile exporté. Le nom de fichier est optionnel avec l'iDRAC version 2.20.20.20 et versions ultérieures.

  REMARQUE : Pour plus d'informations sur les règles d'attribution de nom aux fichiers, voir 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.
- 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.
- 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.

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

    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
- 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 {
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 :

- Un partage réseau (NFS ou CIFS) pris en charge est disponible sur le même sous-réseau que l'iDRAC et le serveur DHCP. Testez le partage réseau pour vous assurer que celui-ci est accessible et que le pare-feu et les autorisations de l'utilisateur sont définis correctement.
- Le profil de configuration de serveur est exporté dans le partage réseau. En outre, assurez-vous que les modifications nécessaires du fichier XML sont terminées, de sorte que les bons paramètres peuvent être appliqués lorsque le processus de Configuration automatique est lancé.
- 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, allez sur **Présentation** > **Paramètres iDRAC** > **Réseau**.
   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 XML 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 XML 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 fonctionnalité de configuration automatique à l'aide de RACADM, utilisez l'objet `iDRAC.NIC.AutoConfig`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Pour plus d'informations sur la fonctionnalité Configuration automatique, voir le livre blanc *Zero-Touch Bare Metal Server Provisioning using Dell iDRAC with Lifecycle Controller Auto Config* (Provisionnement sans intervention de serveurs sans système d'exploitation à l'aide de la configuration automatique de Dell iDRAC avec le Lifecycle Controller) disponible à l'adresse **delltechcenter.com/idrac**.

Utilisation des mots de passe cryptés pour une sécurité optimisée

Vous pouvez définir des mots de passe utilisateur et des mots de passe du BIOS en utilisant un format chiffré à sens unique. 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 créer des hachages SHA256 personnalisés pour définir les mots de passe utilisateur et BIOS d'iDRAC. Cela permet d'inclure les valeurs SHA256 dans le profil de configuration du serveur et sur les interfaces RACADM et WSMAN. Lorsque vous fournissez des valeurs de mot de passe SHA256, vous ne pouvez pas vous authentifier au moyen des protocoles SNMPv3 et IPMI.
- 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 contient les valeurs de hachage requises pour l'authentification SNMPv3. L'importation de ce profil entraîne la perte de l'authentification IPMI pour les utilisateurs pour lesquels les valeurs de mot de passe haché sont définies et l'interface F2 IDRAC indique que le compte d'utilisateur est désactivé.
- Les autres interfaces comme l'interface graphique d'IDRAC montreront que les comptes utilisateur sont activés.

REMARQUE : Lors de la rétrogradation d'un serveur Dell PowerEdge de 12e génération de la version 2.xx.xx.xx à la version 1.xx.xx, si le serveur est configuré avec l'authentification du hachage, vous ne pourrez pas vous connecter à une interface à moins que le mot de passe soit défini sur la valeur par défaut.

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

Chiffrer un mot de passe à l'aide de RACADM

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

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

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 du profil de configuration de serveur, vous pouvez annuler le commentaire de l'attribut de mot de passe existant ou les nouveaux attributs du mot de passe crypté. Si les commentaires des deux sont annulés, une erreur est générée et le mot de passe n'est pas défini. Un attribut portant un commentaire n'est pas appliqué au cours d'une importation.

Génération de mot de passe crypté sans authentification SNMPv3 et IPMI

Pour générer un mot de passe crypté sans authentification SNMPv3 et IPMI :

1. Pour les comptes utilisateur iDRAC, vous devez générer un mot de passe aléatoire à l'aide de SHA256.

   Lorsque vous générez un mot de passe aléatoire, une chaîne binaire de 16 octets est ajoutée. La longueur de la valeur aléatoire doit être de 16 octets, le cas échéant.

2. Fournissez une valeur cryptée et une valeur aléatoire dans le profil de configuration de serveur importé, les commandes RACADM ou WSMAN.
3. 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 iDRAC dont les mots de passe ont été mis à jour avec le cryptage.

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 (Internet Explorer, Firefox, Chrome, ou Safari).
3. Installez le dernier environnement JRE (Java Runtime Environment) (nécessaire si le type de plug-in Java est utilisé pour accéder à iDRAC en utilisant un navigateur web).
4. À partir du DVD *Dell Systems Management Tools and Documentation*, installez RACADM à distance et VMCLI 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 plus d'informations sur RACADM, voir le *guide de référence de l'interface de ligne de commande RACADM d'iDRAC*, disponible à l'adresse **dell.com/idracmanuals.**
5. Installez les éléments suivants en fonction des besoins :
   - Telnet
   - Client SSH
   - TFTP
   - Dell OpenManage Essentials

Concepts associés

Installation et utilisation de l'utilitaire VMCLI , page 254

Tâches associées

Configuration des navigateurs web pris en charge , page 59

Accès à distance à l'iDRAC

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

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

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

Concepts associés

Lancement de la console virtuelle , page 240

Tâches associées

Paramètres réseau , page 41

Installation du système géré

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

- Interface RACADM locale

- Server Administrator

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

Tâches associées

Modification des paramètres du compte d'administrateur local , page 52

Modification des paramètres du compte d'administrateur local

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

1. Dans l'utilitaire de configuration iDRAC, accédez à **Configuration de l'utilisateur**.
   La page **Paramètres iDRAC - Configuration de l'utilisateur** s'affiche.
2. 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 d'iDRAC, accédez à **Présentation** > **Serveur** > **Propriétés** > **Détails**.
   La page **Détails système** s'affiche.
2. Sous **Emplacement du système**, entrez les informations d'emplacement du système géré dans le centre de données.

   Pour plus d'informations sur les options, voir l'*Aide en ligne d'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 définir l'emplacement du système géré, utilisez les objets du groupe `System.Location`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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. Entrez les informations d'emplacement du système géré dans le centre de données. Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les informations sont enregistrées.

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

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

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

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

Pour modifier les paramètres thermiques :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Matériel** > **Ventilateurs** > **Configuration**.
   La page **Configuration du ventilateur** s'affiche.
2. Paramétrez les options suivantes :
   - **Profil thermique** : sélectionnez le profil thermique :
     - **Paramètres de profil thermique par défaut** : suppose que l'algorithme thermique utilise les mêmes paramètres de profil système définis sous **BIOS système** > **Paramètres du BIOS système.Paramètres de profil système**.

     Par défaut, ces paramètres sont réglés 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 la mémoire ou limitation d'UC.
       - Augmentation de la probabilité de l'activation du mode turbo.
       - En général, des vitesses de ventilateur plus élevées à l'état de charges inactif et de contrainte.
     - **Puissance minimale (Performance par watt optimisée)** :
       - Optimisé pour la plus faible consommation énergétique 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.

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

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

     Cette option vous permet de modifier la vitesse des ventilateurs de telle façon que la température d'évacuation ne dépasse pas la limite de température d'évacuation sélectionnée. Elle ne peut pas toujours être garantie dans toutes les conditions de fonctionnement du système d'exploitation en raison d'une dépendance sur la charge du système et les capacités de refroidissement du système.
   - **Décalage de vitesse de ventilateur** : le fait de sélectionner cette option permet 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 être nécessaires. Un décalage de vitesse de ventilateur entraîne l'augmentation de la vitesse des ventilateurs (par le % de décalage) au-delà de la vitesse de référence des ventilateurs calculée par l'algorithme de contrôle thermique. Les valeurs possibles sont les suivantes :
     - **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 vitesse de ventilateur est désactivé. Il s'agit de la valeur par défaut. Lorsque cette option est désactivée, le pourcentage ne s'affiche pas. La valeur de la vitesse de ventilateur par défaut est appliquée sans décalage. À l'inverse, la valeur maximale fait fonctionner tous les ventilateurs à la vitesse maximale.

Le décalage de la vitesse du ventilateur est dynamique et est basée sur le système. L'augmentation de la vitesse du ventilateur de chaque décalage s'affiche en regard de chaque option.

Le décalage de la vitesse du ventilateur augmente toutes les vitesses de ventilateur par le même pourcentage. La vitesse des ventilateurs peut augmenter au-delà de la valeur de décalage en fonction des besoins de refroidissement des composants individuels. La consommation d'énergie globale du système devrait augmenter.

décalage de vitesse de ventilateur vous permet d'augmenter la vitesse des ventilateurs du système avec quatre séquences incrémentielles. Ces étapes sont réparties de manière égale entre la vitesse de référence standard et de la vitesse maximale des ventilateurs du système 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 fonction peut être utilisée pour augmenter le refroidissement à d'autres composants au sein du système.

- **Vitesse du ventilateur minimale en PWN (% du 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 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 la valeur de pourcentage.

  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 d'inactivité et la deuxième valeur est la configuration maximale (qui peut ou non être 100 % selon la configuration du système).

  Les ventilateurs du système peuvent s'exécuter à une vitesse plus élevée que cette vitesse en fonction des besoins thermiques du système mais non à une vitesse inférieure à la vitesse minimale définie. Par exemple, la définition de la Vitesse du ventilateur minimale sur 35 % limite la vitesse du ventilateur de façon à ce qu'elle ne tombe jamais en-dessous de 35 % PWM.

  REMARQUE : 0 % PWM n'indique pas que ventilateur est désactivé. Il s'agit de la plus faible vitesse que le ventilateur peut atteindre.

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 de la réinitialisation du système, cycle d'alimentation, iDRAC ou des mises à jour de BIOS. Certains serveurs Dell peuvent ou non prendre en charge une partie ou l'ensemble de ces options de refroidissement personnalisées 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 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 : 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 8. 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	Pour vérifier le paramètre existant sur le système : `racadm get system.thermalsettings.AirExhaustTemp`

Tableau 8. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple

		• 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)
			Le résultat est :
			`AirExhaustTemp=70`
			Cela signifie que le système est défini de façon à limiter à 70°C la température de sortie d'air.
			Pour définir la limite de température de sortie sur 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 en savoir plus, reportez-vous à l'aide 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.	Valeurs comprises entre 0 et 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal` Une valeur numérique, par exemple 66, est retournée. Cette valeur indique que lorsque

Tableau 8. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple
	• Utilisez l'objet `FanSpeedOffset` pour définir cette valeur à l'aide de la valeur d'index 1.		vous utilisez la commande suivante, elle applique un décalage de vitesse de ventilateur Élevée (66 % PWM) par rapport à la vitesse de ventilateur normale `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 ligne de base
			`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 (ce qui signifie vitesse maximum, 100 % PWM). Généralement, ce décalage entraîne l'augmentation de la vitesse du ventilateur à une vitesse de ventilation 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.	Valeurs comprises entre 0 et 100	`racadm get system.thermalsettings FanSpeedMediumOffsetVal` Ce calcul renvoie une valeur telle que « 47 ». Cela

Tableau 8. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple
	• Utilisez l'objet `FanSpeedOffset` pour définir cette valeur à l'aide de la valeur d'index 2.		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 ligne de base `racadm set system.thermalsettings FanSpeedOffset 2`

`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'indice identifie le décalage à appliquer et les objets `FanSpeedLowOffsetVal`, `FanSpeedMaxOffsetVal`, `FanSpeedHighOffsetVal` et `FanSpeedMediumOffsetVal` (définis antérieurement) sont les valeurs appliquées aux décalages.
		Les valeurs 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`
			Pour définir la valeur du décalage de vitesse de ventilateur sur Élevée (tel que défini dans la section `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	Les valeurs comprises entre 0 et `MFSMaximumLimit` La valeur par défaut est 255 (Aucun)	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.	Les valeurs comprises entre `MFSMinimumLimit` et `MFSMaximumLimit` Lorsque la commande « get » indique une valeur 255,	Pour vous assurer que la vitesse minimum du système ne tombe pas en-dessous de 45 % PWN (45 doit être une valeur comprise

Tableau 8. Paramètres thermiques (suite)

Objet	Description	Utilisation	Exemple
	• 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.	cela signifie que le décalage configuré par l'utilisateur n'est pas appliqué.	entre `MFSMinimumLimit` et `MFSMaximumLimit`) : `racadm set system.thermalsettings.MinimumFanSpeed 45`

`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`
			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. Paramétrez les options suivantes :
   - Profil thermique
   - Limite de température maximale d'évacuation
   - Décalage de la vitesse du ventilateur
   - Vitesse minimum du ventilateur

   Pour plus d'informations sur les champs, voir Modification des paramètres thermiques à l'aide de l'interface Web.

   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 de la réinitialisation du système, cycle d'alimentation, iDRAC ou des mises à jour de BIOS. Certains serveurs Dell peuvent ou non prendre en charge une partie ou l'ensemble de ces options de refroidissement personnalisées 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.

Configuration des navigateurs web pris en charge

REMARQUE : Pour en savoir plus sur les versions de navigateur prises en charge, consultez le fichier de *Notes de mise à jour*, disponible sur **dell.com/idracmanuals**.

La plupart des fonctions de l'interface web d'iDRAC sont accessibles en utilisant ces navigateurs avec leurs paramètres par défaut. Pour certaines fonctions néanmoins, vous devrez modifier quelques paramètres : désactivation des bloqueurs de fenêtres publicitaires, activation de Java, d'ActiveX ou du plug-in HTML5, etc.

Si vous vous connectez à l'interface web d'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 Internet Explorer ou Firefox pour accéder à l'interface web d'iDRAC, vous devrez peut-être configurer certains paramètres comme indiqué dans cette section. Vous pouvez utiliser d'autres navigateurs pris en charge avec leurs paramètres par défaut.

Concepts associés

Affichage des versions localisées de l'interface Web , page 64

Tâches associées

Ajout d'adresse IP de l'iDRAC à la liste des sites de confiance , page 59
Désactivation de la fonction de liste blanche dans Firefox , page 60

Configuration d'Internet Explorer

Cette section fournit des détails à propos de la configuration d'Internet Explorer (IE) pour que vous puissiez accéder et utiliser toutes les fonctionnalités de l'interface Web du contrôleur iDRAC. Ces paramètres sont les suivants :

- Réinitialisation des paramètres de sécurité
- Ajout de l'adresse IP d'iDRAC aux sites de confiance
- Configuration d'IE pour activer la connexion directe SSO Active Directory

Réinitialisation des paramètres de sécurité d'Internet Explorer

Assurez-vous que les paramètres Internet Explorer (IE) sont définis selon les valeurs par défaut recommandées par Microsoft et personnalisez les paramètres comme indiqué dans cette section.

1. Ouvrez IE en tant qu'administrateur ou à l'aide d'un compte d'administrateur.
2. Cliquez sur **Outils Options Internet Sécurité Réseau local** ou **Intranet local**.
3. Cliquez sur **Personnaliser le niveau**, sélectionnez **Moyen-bas**, puis cliquez sur **Réinitialiser**. Cliquez sur **OK** pour confirmer.

Ajout d'adresse IP de l'iDRAC à la liste des sites de confiance

Lorsque vous accédez à l'interface web d'iDRAC, un message vous invite à ajouter l'adresse IP d'iDRAC à la liste des domaines de confiance si l'adresse IP n'y figure pas. Lorsque vous avez terminé, cliquez sur **Actualiser** ou relancez le navigateur web pour établir une connexion à l'interface web d'iDRAC. Si vous n'êtes pas invité à ajouter l'adresse IP, il vous est recommandé d'ajouter l'IP manuellement à la liste des sites de confiance.

REMARQUE : Lorsque vous vous connectez à l'interface web d'iDRAC avec un certificat en lequel le navigateur n'a pas confiance, l'avertissement lié au certificat du navigateur peut apparaître une deuxième fois après que vous avez accusé réception du premier avertissement.

Pour ajouter l'adresse IP d'iDRAC à la liste des sites de confiance :

1. Cliquez sur **Outils** > **Options Internet** > **Sécurité** > **Sites de confiance** > **Sites**.
2. Entrez l'adresse IP d'iDRAC dans **Ajouter ce site web à la zone**.
3. Cliquez successivement sur **Ajouter**, **OK et Fermer**.

4. Cliquez sur **OK**, puis actualisez votre navigateur.

Configuration d'Internet Explorer pour activer la connexion directe Active Directory

Pour configurer les paramètres du navigateur pour Internet Explorer :

1. Dans Internet Explorer, accédez à **Intranet local** et cliquez sur **Sites**.
2. Sélectionnez les options suivantes uniquement :
   - Inclure tous les sites locaux (Intranet) non mentionnés dans d'autres zones.
   - Inclure tous les sites qui n'utilisent pas de serveur proxy.
3. Cliquez sur **Avancé**.
4. Ajoutez tous les noms de domaine relatifs qui seront utilisés pour les instances iDRAC faisant partie de la configuration SSO (par exemple, **myhost.example.com**.)
5. Cliquez sur **Fermer**, puis sur **OK**.

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 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

Désactivation de la fonction de liste blanche dans Firefox

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

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

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

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

Configuration de Firefox pour activer la connexion directe (SSO) Active Directory

Pour configurer les paramètres du navigateur pour Firefox :

1. Dans la barre d'adresses, entrez `about:config`.
2. Dans **Filtre**, entrez `network.negotiate`.
3. Ajoutez le nom 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

Pour utiliser la console virtuelle sur la station de gestion :

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

Pour en savoir plus sur les versions de navigateur prises en charge, consultez le fichier de *Notes de mise à jour* disponible à l'adresse **dell.com/idracmanuals**.

2. Pour utiliser Internet Explorer, configurez Internet Explorer pour **Exécuter en tant qu'administrateur**.
3. Configurez le navigateur Web pour qu'il utilise le plug-in ActiveX, Java ou HTML5.

   La visionneuse ActiveX n'est prise en charge que sur Internet Explorer. Une visionneuse HTML5 ou Java est compatible avec tous les navigateurs.

4. Importez les certificats racine sur le système géré pour éviter les fenêtres contextuelles qui demandent de vérifier les certificats.
5. Installez le module associé **compat-libstdc++-33-3.2.3-61**.

   REMARQUE : Sur Windows, le module associé « compat-libstdc++-33-3.2.3-61 » peut être inclus dans le module .NET ou le module du système d'exploitation.

6. Si vous utilisez un système d'exploitation MAC, sélectionnez l'option **Activer l'accès aux périphériques d'aide** dans la fenêtre **Accès universel**.

   Pour en savoir plus, voir la documentation du système d'exploitation MAC.

Concepts associés

Configuration d'Internet Explorer pour qu'il utilise le plug-in HTML5 , page 61
Configuration du navigateur Web pour utiliser le plug-in Java , page 61
Configuration d'IE pour qu'il utilise le plug-in ActiveX , page 62
Importation de certificats CA vers la station de gestion , page 63

Configuration d'Internet Explorer pour qu'il utilise le plug-in HTML5

La console virtuelle et les API de médias virtuels HTML5 sont créées à l'aide de la technologie HTML5, dont voici les avantages :

- L'installation n'est pas nécessaire sur le poste de travail client.
- La compatibilité est basée sur le navigateur et non pas sur le système d'exploitation ou les composants installés.
- Compatible avec la plupart des ordinateurs de bureau et des plateformes mobiles.
- Déploiement rapide et le client est téléchargé dans le cadre d'une page web.

Vous devez configurer les paramètres d'Internet Explorer (IE) pour pouvoir lancer et exécuter la console virtuelle et les applications de médias virtuels, toutes basées sur HTML5. Pour configurer les paramètres du navigateur :

1. Désactivez le bloqueur de fenêtres publicitaires intempestives. Pour ce faire, cliquez sur **Outils** > **Options Internet** > **Confidentialité** et désélectionnez la case **Activer le bloqueur de fenêtres publicitaires intempestives**.
2. Vous pouvez démarrer la console virtuelle HTML5 à l'aide de l'une des méthodes suivantes :
   - Dans IE, cliquez sur **Outils** > **Paramètres d'affichage de compatibilité** et désélectionnez la case **Afficher les sites intranet dans l'affichage de compatibilité**.
   - Dans IE utilisant une adresse IPv6, modifiez l'adresse IPv6 comme suit :

     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/ to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/
     ```

   - Dirigez la console virtuelle HTML5 dans IE utilisant une adresse IPv6, modifiez l'adresse IPv6 comme suit :

     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/console to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/console
     ```

3. Pour afficher les informations de la barre de titre dans IE, allez à **Panneau de configuration** > **Apparence et personnalisation** > **Personnalisation** > **Fenêtre classique**

Configuration du navigateur Web pour utiliser le plug-in Java

Installez un environnement JRE (Java Runtime Environment) si vous utilisez Firefox ou IE et voulez utiliser le visualiseur Java.

REMARQUE : Installez une version JRE 32 bits ou 64 bits sur un système d'exploitation 64 bits ou une version 32 bits sur un système d'exploitation 32 bits.

Pour configurer IE pour utiliser le plug-in Java :

- Désactivez les invites automatiques des téléchargements de fichiers dans Internet Explorer.
- Désactivez le *mode de sécurité renforcée* dans Internet Explorer.

Concepts associés

Configuration de la console virtuelle , page 239

Configuration d'IE pour qu'il utilise le plug-in ActiveX

Vous devez configurer les paramètres du navigateur Internet Explorer avant de lancer et d'exécuter les applications Console virtuelle et Média virtuel à base ActiveX. Les applications ActiveX sont délivrées comme fichiers CAB signés issus du serveur iDRAC. Si le type de plug-in est défini sur ActiveX natif dans la console virtuelle, lorsque vous tentez de démarrer la console virtuelle, le fichier CAB est téléchargé sur le système client et la console virtuelle ActiveX est lancée. Internet Explorer exige certaines configurations pour télécharger, installer et exécuter ces applications ActiveX.

Internet Explorer est disponible en versions 32 bits et 64 bits sur les navigateurs 64 bits. Vous pouvez utiliser n'importe quelle version, mais si vous installez le plug-in du navigateur 64 bits, puis que vous essayez d'exécuter la visionneuse dans un navigateur 32 bits, vous devez installer le plug-in de nouveau.

REMARQUE : Vous pouvez utiliser le plug-in ActiveX uniquement avec Internet Explorer.

REMARQUE : Pour utiliser le plug-in ActiveX sur les systèmes dotés d'Internet Explorer 9, avant de configurer Internet Explorer, assurez-vous de désactiver le mode de sécurité renforcée dans Internet Explorer ou dans le gestionnaire de serveur des systèmes d'exploitation Windows Server.

Dans le cas des applications ActiveX sous Windows 2003, Windows XP, Windows Vista, Windows 7 et Windows 2008, configurez les paramètres Internet Explorer suivants de sorte à utiliser le plug-in ActiveX :

1. Effacez le cache du navigateur.
2. Ajoutez l'adresse IP ou le nom d'hôte d'iDRAC à la liste des **Sites de confiance**.
3. Réinitialisez les paramètres personnalisés pour les ramener à **Moyen bas** ou chargez les paramètres pour autoriser l'installation des plug-ins ActiveX signés.
4. Autorisez le navigateur à télécharger le contenu crypté et activer les extensions tierces du navigateur. Pour ce faire, accédez à **Outils** > **Options Internet** > **Avancé**, désélectionnez l'option **Ne pas enregistrer les pages cryptées sur le disque** et sélectionnez l'option **Activer les extensions tierces du navigateur**.

   REMARQUE : Redémarrez Internet Explorer pour appliquer le paramètre Activer les extensions tierce partie du navigateur.

5. Accédez à **Outils** > **Options Internet** > **Sécurité** et sélectionnez le fuseau horaire lors duquel vous voulez exécuter l'application.
6. Cliquez sur **Niveau personnalisé**. Dans la fenêtre **Paramètres de sécurité**, procédez comme suit :
   - Sélectionnez **Activé** pour **Demander confirmation pour les contrôles ActiveX**.
   - Sélectionnez **Demander** pour **Télécharger les contrôles ActiveX signés**.
   - Sélectionnez **Activé** ou **Demander** pour **Exécuter les contrôles ActiveX et les plug-ins**.
   - Sélectionnez **Activé** ou **Demander** pour **Contrôles ActiveX reconnus sûrs pour l'écriture de scripts.**
7. Cliquez sur **OK** pour fermer la fenêtre **Paramètres de sécurité**.
8. Cliquez sur **OK** pour fermer la fenêtre **Options Internet**.

   REMARQUE : Sur les systèmes dotés d'Internet Explorer 11, assurez-vous d'ajouter l'IP iDRAC en cliquant sur **Outils** > **Paramètres d'affichage de compatibilité**.

   REMARQUE :
   - Les diverses versions d'Internet Explorer partagent les mêmes **Options Internet**. Par conséquent, une fois que vous avez ajouté le serveur à la liste des *sites de confiance* pour un navigateur, les autres navigateurs utilisent le même paramètre.
   - Avant d'installer le contrôle ActiveX, Internet Explorer peut afficher un avertissement de sécurité. Pour terminer l'installation d'ActiveX, acceptez le contrôle ActiveX lorsque Internet Explorer affiche un avertissement de sécurité.

Concepts associés

Effacement du cache du navigateur , page 63
Paramètres supplémentaires pour les systèmes d'exploitation Windows Vista ou Microsoft les plus récents , page 63

Paramètres supplémentaires pour les systèmes d'exploitation Windows Vista ou Microsoft les plus récents

Les navigateurs Internet Explorer intégrés à Windows Vista ou aux systèmes d'exploitation les plus récents sont dotés d'une fonction de sécurité supplémentaire appelée *Mode protégé*.

Pour lancer et exécuter des applications ActiveX dans les navigateurs Internet Explorer avec le *mode protégé* :

1. Exécutez IE en tant qu'administrateur.
2. Accédez à **Outils** > **Options Internet** > **Sécurité** > **Sites de confiance**.
3. Veillez à ne pas sélectionner l'option **Activer le mode protégé** dans la zone Sites de confiance. Vous pouvez également ajouter l'adresse iDRAC aux sites dans la zone Intranet. Par défaut, le mode protégé est désactivé dans la zone Intranet et la zone Sites de confiance.
4. Cliquez sur **Sites**.
5. Dans le champ **Ajouter ce site Web à la zone**, ajoutez l'adresse de votre iDRAC et cliquez sur **Ajouter**.
6. Cliquez sur **Fermer**, puis sur **OK**.
7. Fermez et redémarrez le navigateur pour appliquer les paramètres.

Effacement du cache du navigateur

Si vous rencontrez des problèmes lors de l'utilisation de la console virtuelle (erreurs hors plage, problèmes de synchronisation, etc.), effacez la mémoire cache du navigateur pour retirer ou supprimer les anciennes versions du Visualiseur susceptibles d'être stockées sur le système, puis réessayez.

REMARQUE : Vous devez disposer du privilège Administrateur pour pouvoir effacer la mémoire cache du navigateur.

Suppression des versions Java précédentes

Pour supprimer les anciennes versions du visualiseur Java sous Windows ou Linux, procédez comme suit :

1. Dans l'invite de commande, exécutez `javaws-viewer` ou `javaws-uninstall`
   Le **visualiseur Java Cache** s'affiche.
2. Supprimez les éléments intitulés *Client de console virtuelle iDRAC.*

Importation de certificats CA vers la station de gestion

Lorsque vous lancez la console virtuelle ou Média Virtuel, des invites s'affichent pour vérifier les certificats. Si vous utilisez des certificats de serveur Web personnalisés, vous pouvez éviter ces invites en important les certificats vers la banque de certificats de confiance Java ou ActiveX.

Concepts associés

Importation d'un certificat CA vers le magasin de certificats de confiance Java , page 63
Importation d'un certificat CA dans le magasin de certificats de confiance ActiveX , page 64

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 du **Panneau de configuration Java** se ferme.

Importation d'un certificat CA dans le magasin de certificats de confiance ActiveX

Vous devez utiliser l'outil de ligne de commande SSL OpenSSL pour créer le hachage de certificat en utilisant SHA (Secure Hash Algorithm). Il est recommandé d'utiliser l'outil OpenSSL 1.0.x ou une version suivante, car il utilise SHA par défaut. Le certificat CA doit être au format PEM codé en base 64. Il s'agit d'un processus à exécution unique pour importer chaque certificat CA.

Pour importer le certificat CA dans la banque de certificats de confiance ActiveX :

1. Ouvrez l'invite de commande OpenSSL.
2. Exécutez un hachage de 8 octets sur le certificat CA en cours d'utilisation sur la station de gestion à l'aide de la commande `openssl x509 -in (nome de cert CA) -noout -hash`

   Un fichier de sortie est généré. Par exemple, si le fichier de certificat CA s'appelle **cacert.pem**, la commande est la suivante :

   ```
   openssl x509 -in cacert.pem -noout -hash
   ```

   Une sortie similaire à « 431db322 » est générée.
3. Renommez le fichier de certificat en utilisant le nom du fichier de sortie et incluez l'extension « 0 ». Par exemple, 431db322.0.
4. Copiez le certificat CA renommé dans votre répertoire de base. Par exemple, **C:\Documents and Settings\<utilisateur>**.

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

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

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

Mise à jour du micrologiciel de périphérique

Avec iDRAC, vous pouvez mettre à jour les micrologiciels d'iDRAC, du BIOS et des périphériques pris en charge à l'aide de la mise à jour Lifecycle Controller, tels que :

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

PRÉCAUTION : La mise à jour du micrologiciel 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 mise à jour du micrologiciel du bloc d'alimentation.

Vous devez charger le micrologiciel requis vers l'iDRAC. Une fois le chargement terminé, la version du micrologiciel actuellement installée sur le périphérique et la version en cours d'application sont affichées. Si la version du micrologiciel en cours d'application 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.

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

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

- `.exe` : Dell Update Package (DUP) à base Windows
- `.d7` : contient les micrologiciels iDRAC et Lifecycle Controller.

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

Pour les fichiers dont l'extension est `.d7`, vous devez disposer du privilège de configuration.

REMARQUE : Après la mise à niveau du micrologiciel de l'iDRAC, il se peut que vous constatiez une différence dans l'horodatage affiché dans le journal du Lifecycle Controller jusqu'à ce que l'heure de l'iDRAC soit réinitialisée à l'aide du protocole NTP. Le journal Lifecycle affiche l'heure du BIOS jusqu'à ce que l'heure de l'iDRAC soit réinitialisée.

Vous pouvez effectuer les mises à jour du micrologiciel 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 ou HTTP ou à un référentiel réseau qui contient les packages DUP Windows et un fichier de catalogue correspondant.

  Vous pouvez créer des logithèques personnalisées à l'aide du Gestionnaire de logithèques Dell. Pour des informations supplémentaires, voir le *Dell Repository Manager Data Center User's Guide* (*Guide d'utilisation du datacenter du Gestionnaire de logithèques)*. L'iDRAC peut fournir un rapport sur les différences entre le BIOS et le micrologiciel installé sur le système, ainsi que sur les mises à jour disponibles dans la logithèque. Toutes les mises à jour applicables contenues dans la logithèque s'appliquent au système. Cette fonction est disponible avec la licence iDRAC Enterprise.

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

Plusieurs outils et interfaces permettent de mettre à jour le micrologiciel iDRAC. Le tableau suivant s'applique uniquement au micrologiciel 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 micrologiciel.

Tableau 9. Types de fichiers d'image et dépendances

	Image .D7		DUP iDRAC	
Interface	**Pris en charge**	**Nécessite LC activé**	**Pris en charge**	**Nécessite LC activé**
Utilitaire BMCFW64.exe	Oui	Non	Non	S/O
Racadm FWupdate (ancien)	Oui	Non	Non	S/O
Racadm Update (nouveau)	Oui	Oui	Oui	Oui
UI iDRAC	Oui	Oui	Oui	Oui
WSMAN	Oui	Oui	Oui	Oui
DUP OS intrabande	Non	S/O	Oui	Non

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

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

Tableau 10. Mise à jour du micrologiciel

Nom de composant	Restauration du micrologiciel prise en charge ? (Oui ou Non)	Hors bande : redémarrage du système requis ?	Intrabande : redémarrage du système requis ?	Interface utilisateur graphique de Lifecycle Controller : redémarrage requis ?
Diagnostics	Non	Non	Non	Non
Pack de pilotes du système d'exploitation	Non	Non	Non	Non
iDRAC avec Lifecycle Controller	Oui	Non	**Non*	Oui
BIOS	Oui	Oui	Oui	Oui
Contrôleur RAID	Oui	Oui	Oui	Oui
Fonds de panier	Oui	Oui	Oui	Oui
Enceintes	Oui	Oui	Non	Oui
Carte réseau	Oui	Oui	Oui	Oui
Bloc d'alimentation	Oui	Oui	Oui	Oui
CPLD	Non	Oui	Oui	Oui
Cartes FC	Oui	Oui	Oui	Oui
Disques SSD PCIe NVMe (serveurs Dell PowerEdge de 13e génération uniquement)	Oui	Non	Non	Non
Disques durs SAS/SATA	Non	Oui	Oui	Non
CMC (sur les serveurs PowerEdge FX2)	Non	Oui	Oui	Oui
OS Collector (Collecteur de système d'exploitation)	Non	Non	Non	Non

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

** Lorsque l'iDRAC est mis à jour à partir de la version 1.30.30 ou ultérieure, un redémarrage du système n'est pas nécessaire. Cependant, pour les micrologiciels iDRAC de version antérieure à 1.30.30, le redémarrage du système est nécessaire si la mise à jour est effectuée via une interface hors bande.

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.

Lorsque vous recherchez les mises à jour, si une version est marquée comme étant **Available (Disponible)** cela n'indique pas toujours qu'il s'agit de la dernière version disponible. Avant d'installer la mise à jour, assurez-vous que la version que vous choisissez d'installer est plus récente que la version actuellement installée. Si vous souhaitez contrôler la version que l'iDRAC détecte, créez une logithèque personnalisée à l'aide de Dell Repository Manager (DRM) et configurez l'iDRAC pour utiliser cette logithèque pour rechercher des mises à jour.

Tâches associées

Mise à jour du micrologiciel d'un seul périphérique , page 67
Mise à jour du micrologiciel via l'espace de stockage , page 67
Mise à jour du micrologiciel à l'aide de FTP, de TFTP ou de HTTP , page 68
Mise à jour du micrologiciel de périphérique à l'aide de RACADM , page 69
Planification des mises à jour automatiques du micrologiciel , page 69
Mise à jour du micrologiciel à l'aide de l'interface Web CMC , page 71
Mise à jour du micrologiciel à l'aide de DUP , page 71

Mise à jour du micrologiciel à l'aide de l'interface RACADM , page 71
Mise à jour du micrologiciel à l'aide des Lifecycle Controller Remote Services , page 72

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

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

REMARQUE : CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.

Mise à jour du micrologiciel d'un seul périphérique

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

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

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

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

   Si le fichier d'image du micrologiciel est valide et a été chargé avec succès, la colonne **Contenu** affiche une icône « plus » (+) à côté du nom du fichier d'image du micrologiciel. Développez le nom pour afficher le **Nom du périphérique** et les informations des versions du micrologiciel **Actuelle** et **Disponibles**.
5. Sélectionnez le fichier de micrologiciel requis et effectuez l'une des opérations suivantes :
   - Pour les images de micrologiciel qui n'exigent pas de redémarrage du système hôte, cliquez sur **Installer** (par exemple, le fichier micrologiciel iDRAC).
   - Pour les images de micrologiciel qui nécessitent un redémarrage du système hôte, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**.
   - Pour annuler la mise à jour du micrologiciel, cliquez sur **Annuler**.

   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 travaux**, cliquez sur **File d'attente des travaux**. Cette page permet d'afficher et de gérer les mises à jour différées du micrologiciel ou cliquez sur **OK** pour actualiser la page et afficher l'état de la mise à jour du micrologiciel.

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

Concepts associés

Mise à jour du micrologiciel de périphérique , page 64
Affichage et gestion des mises à jour planifiées , page 73

Mise à jour du micrologiciel via l'espace de stockage

Un référentiel est un emplacement de stockage qui permet de stocker les packages de mise à jour et d'y accéder. Dell Repository Manager (DRM) vous permet de créer et de gérer un référentiel dans lequel iDRAC peut rechercher des mises à jour. La création et l'utilisation de référentiels de mise à jour de firmware personnalisés présentent plusieurs avantages, car cela permet de choisir les périphériques ou les composants à mettre à jour. À l'aide d'iDRAC, vous pouvez effectuer une mise à jour de l'espace de stockage en mode surveillé ou entièrement surveillé.

REMARQUE : Il est recommandé d'utiliser Dell Repository Manager pour effectuer des mises à jour sur votre système au lieu de télécharger et de mettre à jour le firmware directement à partir du site Web de Dell.

DRM peut utiliser les éléments suivants pour créer le référentiel :

- le nouveau catalogue en ligne Dell
- Catalogue Dell précédemment utilisé
- le référentiel source local
- un référentiel personnalisé

REMARQUE : Pour en savoir plus sur DRM, voir **delltechcenter.com/repositorymanager**.

REMARQUE : Lifecycle Controller doit être activé et vous devez disposer des privilèges de contrôle du serveur pour mettre à jour le firmware pour les périphériques autres qu'iDRAC.

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

1. Dans l'interface web d'iDRAC, allez à **Présentation** > **Paramètres iDRAC** > **Mise à jour et restauration**.
   La page **Mise à jour de micrologiciel** s'affiche.
2. Sur l'onglet **Mise à jour**, sélectionnez **Partage réseau** comme **emplacement des fichiers**.
3. Dans la section **Emplacement du catalogue**, entrez les détails de paramétrage du réseau.

   Lorsque vous indiquez les paramètres de partage du 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, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
4. Cliquez sur **Rechercher les mises à jour**.

   La section **Détails de la mise à jour** affiche un rapport de comparaison montrant les versions actuelles du micrologiciel et les versions de micrologiciel disponibles dans le référentiel.

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

   REMARQUE : Une version marquée comme disponibles n'indique pas toujours qu'il s'agit de la dernière version disponible ou plus récente que la version déjà installée.

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

   Lorsque vous cliquez sur **Installer**, **Installer et redémarrer** ou **Installer au prochain redémarrage**, le message `Updating Job Queue` s'affiche.
6. Cliquez sur la page **File d'attente des travaux** pour afficher la page **File d'attente des travaux**. Cette page permet d'afficher et de gérer les mises à jour différées du micrologiciel ou cliquez sur **OK** pour actualiser la page et afficher l'état de la mise à jour du micrologiciel.

Concepts associés

Mise à jour du micrologiciel de périphérique , page 64
Affichage et gestion des mises à jour planifiées , page 73
Planification des mises à jour automatiques du micrologiciel , page 69

Mise à jour du micrologiciel à l'aide de FTP, de TFTP ou de HTTP

Vous pouvez configurer un serveur FTP, TFTP ou HTTP et configurer iDRAC pour qu'il puisse l'utiliser afin d'effectuer les mises à jour du micrologiciel. Vous pouvez utiliser les packages de mise à jour Windows (DUP) et un fichier de catalogue.

REMARQUE : Lifecycle Controller doit être activé et vous devez disposer des privilèges de contrôle du serveur pour mettre à jour le micrologiciel pour les périphériques autres que l'iDRAC.

1. Dans l'interface web d'iDRAC, allez à **Présentation** > **Paramètres iDRAC** > **Mise à jour et restauration**.
   La page **Mise à jour de micrologiciel** s'affiche.
2. Dans l'onglet **Mise à jour**, sélectionnez l'option de votre choix dans **Emplacement de fichier** –**FTP**, **TFTP** ou **HTTP**.
3. Entrez les informations requises dans les champs qui s'affichent.

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

4. Cliquez sur **Vérifier les mises à jour**.
5. Une fois le téléversement terminé, la section **Détails de la mise à jour** affiche un rapport de comparaison montrant les versions actuelles du micrologiciel et celles disponibles dans le référentiel.

   REMARQUE : Les mises à jour qui ne sont pas prises en charge ou qui ne sont pas applicables au système ou au matériel installé ne figurent pas dans le rapport de comparaison.

6. Sélectionnez les mises à jour requises et effectuez l'une des opérations suivantes :
   - Pour les images de micrologiciel qui ne nécessitent pas un redémarrage du système hôte, cliquez sur **Installer**. Par exemple, le fichier micrologiciel `.d7`.
   - Pour les images de micrologiciel qui nécessitent un redémarrage du système hôte, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**.
   - Pour annuler la mise à jour du micrologiciel, cliquez sur **Annuler**.

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

7. **File d'attente des tâches pour afficher la** page, cliquez sur **File d'attente des tâches**. Sur cette page, vous pouvez afficher et gérer les mises à jour de micrologiciel différées. Cliquez sur **OK** pour actualiser la page et afficher l'état de la mise à jour du micrologiciel.

Concepts associés

Mise à jour du micrologiciel de périphérique , page 64
Affichage et gestion des mises à jour planifiées , page 73
Planification des mises à jour automatiques du micrologiciel , page 69

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

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

Exemples :

- Pour générer un rapport de comparaison à l'aide d'un espace de stockage de mise à jour :

```
racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verifycatalog
```

- Pour exécuter toutes les mises à jour applicables à partir d'un espace de stockage de mise à jour en utilisant `myfile.xml` sous la forme d'un fichier de catalogue et effectuer un redémarrage normal :

```
racadm update -f "myfile.xml" -b "graceful" -l //192.168.1.1 -u test -p passwd
```

- Pour exécuter toutes les mises à jour applicables à partir d'un espace de stockage de mise à jour FTP à l'aide de `Catalog.xml` sous la forme d'un fichier de catalogue :

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

Planification des mises à jour automatiques du micrologiciel

Vous pouvez créer une planification périodique selon laquelle l'iDRAC vérifie les nouvelles mises à jour du micrologiciel. Au jour et à l'heure planifiés, l'iDRAC se connecte à la destination spécifiée, vérifie l'existence de nouvelles mises à jour et applique ou diffère les mises à jour applicables. Un fichier journal est créé sur le serveur distant, qui contient des informations sur l'accès au serveur et les mises à jour échelonnées du micrologiciel.

Il est recommandé de créer un référentiel à l'aide de Dell Repository Manager (DRM) et de configurer l'iDRAC pour utiliser ce référentiel afin de rechercher et effectuer les mises à jour du micrologiciel. Utiliser un référentiel interne vous permet de contrôler le micrologiciel et les versions disponibles pour l'iDRAC et permet d'éviter toute modification non prévue du micrologiciel.

REMARQUE : Pour en savoir plus sur DRM, voir **delltechcenter.com/repositorymanager**.

Une licence iDRAC Enterprise est requise pour la planification de mises à jour automatiques.

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

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

Concepts associés

Mise à jour du micrologiciel de périphérique , page 64
Affichage et gestion des mises à jour planifiées , page 73

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

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

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

1. Dans l'interface Web iDRAC, allez à **Présentation** > **Paramètres iDRAC** > **Mise à jour et restauration** .
   La page **Mise à jour de micrologiciel** s'affiche.
2. Cliquez sur l'onglet **Mise à jour automatique**.
3. Sélectionnez l' option de **sélection de la mise à jour automatique**.
4. Sélectionnez l'une ou l'autre des options suivantes pour indiquer si le redémarrage d'un système est requis après la préparation des mises à jour :
   - **Planifier des mises à jour** : effectuez des mises à jour de micrologiciel sans redémarrer le serveur.
   - **Planifier des mises à jour et redémarrer le serveur** : permet de redémarrer le serveur après la programmation des mises à jour de micrologiciel.
5. Sélectionnez un des éléments suivants pour spécifier l'emplacement des images du micrologiciel :
   - **Réseau** : utilisez le fichier de catalogue depuis un partage réseau (CIFS ou NFS). Saisissez les détails de l'emplacement du partage réseau.
     REMARQUE : Lorsque vous indiquez les paramètres de partage du 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.
   - **FTP** - Utilisez le fichier de catalogue à partir du site FTP. Saisissez les détails du site FTP.
6. En fonction de la sélection à l'étape 5, entrez les paramètres réseau ou les paramètres FTP.
   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
7. Dans la section **Mise à jour de la fenêtre de planification**, spécifiez l'heure de début de la mise à jour de micrologiciel et la fréquence des mises à jour (tous les jours, toutes les semaines ou tous les mois).
   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
8. Cliquez sur **Planifier la mise à jour**.
   La prochaine tâche planifiée est créée dans la file d'attente des tâches. Cinq minutes après le début de la première instance des tâches récurrentes, la tâche de la prochaine période est créée.

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

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

- Pour activer la mise à jour automatique du micrologiciel :

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
```

- Pour afficher l'état de la mise à jour automatique du micrologiciel :

```
racadm get lifecycleController.lcattributes.AutoUpdate
```

- Pour planifier l'heure de début et la fréquence de la mise à jour de micrologiciel :

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

Par exemple :

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

```
racadm AutoUpdateScheduler create -u admin -p pwd -l //1.2.3.4/CIFS-share -f cat.xml
-time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- Pour mettre à jour automatiquement le micrologiciel à l'aide de FTP :

```
racadm AutoUpdateScheduler create -u admin -p pwd -l ftp.mytest.com -pu puser -pp puser
-po 8080 -pt http -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- Pour afficher le calendrier de mise à jour du micrologiciel en cours :

```
racadm AutoUpdateScheduler view
```

- Pour désactiver la mise à jour automatique du micrologiciel :

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
```

- Pour effacer les détails de planification :

```
racadm AutoUpdateScheduler clear
```

Mise à jour du micrologiciel à l'aide de l'interface Web CMC

Vous pouvez mettre à jour le micrologiciel d'iDRAC des serveurs lames à l'aide de l'interface Web CMC.

Pour mettre à jour le micrologiciel d'iDRAC en utilisant l'interface de Web CMC :

1. Ouvrez une session dans l'interface Web CMC.
2. Allez sous **Serveur** > **Présentation** > **<nom du serveur>**.
   La page **Condition du serveur** s'affiche.
3. Cliquez sur **Lancer l'interface Web iDRAC** et **Mise à jour du micrologiciel iDRAC**.

Concepts associés

Mise à jour du micrologiciel de périphérique , page 64
Mise à niveau du micrologiciel à l'aide de l'interface Web d'iDRAC , page 67

Mise à jour du micrologiciel à l'aide de DUP

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

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

  REMARQUE : Lors de la mise à jour du micrologiciel 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`

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

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

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

TFTP server:

- 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.d7`.

- 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.d7`.

- 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 référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Mise à jour du micrologiciel à l'aide des Lifecycle Controller Remote Services

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

Mise à jour du micrologiciel CMC à partir de l'iDRAC

Dans les châssis PowerEdge FX2/FX2s, vous pouvez mettre à jour le micrologiciel du CMC (Contrôleur de gestion de châssis) et tout composant pouvant être mis à jour par le CMC et partagé par les serveurs à partir de l'iDRAC.

Avant d'appliquer la mise à jour, assurez-vous que :

- Les serveurs ne sont pas autorisés à se mettre sous tension par le CMC.
- Les châssis avec écran LCD doivent afficher un message indiquant que « la mise à jour est en cours ».
- Le châssis sans écran LCD doit indiquer la progression de la mise à jour à l'aide du schéma de clignotement de la LED.
- Au cours de la mise à jour, les commandes d'alimentation des actions de châssis sont désactivées.

Les mises à jour des composants tels que la PSoC (Programmable System-on-Chip) de module d'E/S exigent que tous les serveurs soient à l'état inactif, la mise à jour est appliquée au cours du prochain cycle de mise sous tension du châssis.

Paramétrage du CMC pour effectuer la mise à jour du micrologiciel du CMC depuis l'iDRAC

Dans les châssis PowerEdge FX2/FX2s, avant d'effectuer la mise à jour du micrologiciel depuis l'iDRAC pour le CMC et ses composants partagés, procédez comme suit :

1. Lancez l'interface Web du CMC
2. Accédez à **Présentation du châssis** > **Configuration** > **Généralités**.
3. Depuis le menu déroulant **Gestion du châssis en mode serveur**, sélectionnez **Gérer et surveiller**, puis cliquez sur **Appliquer**.

Paramétrage d'iDRAC pour effectuer la mise à jour du micrologiciel de CMC

Dans les châssis PowerEdge FX2/FX2s, avant de mettre à jour le micrologiciel de CMC et ses composants partagés à partir de l'iDRAC, effectuez les paramétrages suivants dans l'iDRAC :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation générale** > **Paramétrage d'iDRAC** > **Mise à jour et restauration** > **Paramètres**
   La page **Paramètres de mise à jour de Chassis Management Controller** s'affiche.
2. Pour **Autoriser les Mises à jour de CMC via le système d'exploitation et le Lifecycle Controller**, sélectionnez **Activé** pour activer la mise à jour du micrologiciel du CMC à partir de l'iDRAC.
3. Sous **Paramètres CMC actuels**, assurez-vous que l'option **Chassis Management en mode Serveur** affiche **Gérer et surveiller**. Vous pouvez la définir dans le CMC.

Affichage et gestion des mises à jour planifiées

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

Tâches associées

Mise à jour du micrologiciel de périphérique , page 64

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

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

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

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

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

Pour afficher les mises à jour différées à l'aide de RACADM, utilisez la sous-commande `jobqueue`. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Restauration du micrologiciel du périphérique

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

Sur les serveurs Dell PowerEdge de 13e génération dotés des mêmes micrologiciels iDRAC et Lifecycle Controller, la restauration du micrologiciel iDRAC restaure également le micrologiciel Lifecycle Controller. Toutefois, sur un serveur PowerEdge de 12e génération doté du micrologiciel version 2.*xx.xx.xx*, la restauration d'iDRAC vers une version précédente comme 1.*xx.xx* n'annule pas la version de Lifecycle Controller. Il est recommandé de restaurer une version antérieure du Lifecycle Controller après avoir restauré une version antérieure de l'iDRAC.

REMARQUE : Sur un serveur PowerEdge de 12e génération doté du micrologiciel de version 2.10.10.10, vous ne pouvez pas restaurer la version 1.*xx.xx* du Lifecycle Controller sans restaurer l'iDRAC. Vous devez revenir d'abord à la version 1.*xx.xx*. Vous pouvez alors restaurer une version antérieure du Lifecycle Controller.

Il est recommandé de garder le micrologiciel mis à jour pour être sûr de disposer des fonctionnalités et mises à jour de sécurité les plus récentes. Vous aurez peut-être besoin d'annuler une mise à jour et de revenir à une version antérieure si vous rencontrez des problèmes après une mise à jour. Pour installer une version antérieure, utilisez Lifecycle Controller pour rechercher les mises à jour et sélectionnez la version que vous souhaitez installer.

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

- iDRAC avec Lifecycle Controller
- BIOS
- Carte d'interface réseau (NIC)
- Unité d'alimentation (PSU)
- Contrôleur RAID
- Fond de panier

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

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

- Vous disposez des droits de configuration nécessaires pour restaurer le micrologiciel d'iDRAC.
- Vous disposez des droits de contrôle du serveur et avez activé le Lifecycle Controller pour la restauration de micrologiciel 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 micrologiciel en utilisant n'importe laquelle des méthodes suivantes :

- Interface web iDRAC
- Interface web CMC
- CLI RACADM – iDRAC et CMC
- GUI de Lifecycle Controller
- les services à distance Lifecycle Controller.

Tâches associées

Restauration du micrologiciel à l'aide de l'interface Web d'iDRAC , page 74
Restauration du micrologiciel à l'aide de l'interface Web CMC , page 75
Restauration du micrologiciel à l'aide de l'interface RACADM , page 75
Restauration du micrologiciel à l'aide du Lifecycle Controller , page 75
Restauration du micrologiciel à l'aide des services distants Lifecycle Controller , page 75

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

Pour restaurer un micrologiciel de périphérique :

1. Dans l'interface Web iDRAC, allez dans **Présentation** > **Paramètres iDRAC** > **Mise à jour et restauration** > **Restauration**.
   Tous les périphériques pour lesquels vous pouvez restaurer le micrologiel s'affichent dans la page de **Restauration**. Vous pouvez afficher le nom du périphérique, les périphériques associés, la version du micrologiciel actuellement installé, ainsi que la version de restauration du micrologiciel disponible.
2. Sélectionnez un ou plusieurs périphériques pour lesquels vous voulez restaurer le micrologiciel.
3. Selon les périphériques sélectionnés, cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**. Si seul l'iDRAC est sélectionné, cliquez sur **Installer**.
   Lorsque vous cliquez sur **Installer et redémarrer** ou **Installer au prochain redémarrage**, le message « Mise à jour de la file d'attente des tâches » s'affiche.
4. Cliquez sur **File d'attente des tâches**.
   La page **File d'attente des tâches** qui s'affiche vous permet d'afficher et de gérer les mises à jour du micrologiciel par étapes.

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

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

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

Restauration du micrologiciel à l'aide de l'interface Web CMC

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

1. Ouvrez une session dans l'interface Web CMC.
2. Accédez à **Présentation du serveur** > **<nom du serveur>**.
   La page **Condition du serveur** s'affiche.
3. Cliquez sur **Lancer l'iDRAC** et effectuez la restauration du micrologiciel du périphérique tel que mentionné dans la section Restauration du micrologiciel à l'aide de l'interface Web de l'iDRAC.

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
   ```

   La `Rollback Versio` du périphérique dont vous voulez restaurer le micrologiciel doit être `Available`. De plus, notez le FQDD.

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

   ```
   racadm rollback <FQDD>
   ```

   Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Restauration du micrologiciel à l'aide du Lifecycle Controller

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

Restauration du micrologiciel à l'aide des services distants Lifecycle Controller

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

Restauration d'iDRAC

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

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

Utilisation du serveur TFTP

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

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

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

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

Sauvegarde du profil du serveur

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

REMARQUE : CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.

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

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

REMARQUE : Dans les serveurs de 13e génération, cette fonction est activée automatiquement.

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

- La fonction Collecter l'inventaire système au redémarrage (CSIOR) est activée. Si vous lancez une opération de restauration pendant que la fonction CSIOR est désactivée, le message suivant s'affiche :

```
System Inventory with iDRAC may be stale,start CSIOR for updated inventory
```

- Pour effectuer la sauvegarde sur une carte SD vFlash :
  - La carte SD vFlash est insérée, activée et initialisée.
  - La carte SD vFlash dispose d'au moins 100 Mo d'espace libre pour stocker le fichier de sauvegarde.

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

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

Concepts associés

Planification de la sauvegarde automatique du profil de serveur , page 77
Importation du profil du serveur , page 78

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

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

1. Accédez à **Présentation générale** > **Paramètres iDRAC** > **Profil du serveur**.
   La page **Sauvegarde et exportation du profil du serveur** s'affiche.
2. Sélectionnez un des éléments suivants pour enregistrer l'image du fichier de sauvegarde :
   - **Réseau** pour enregistrer l'image du fichier de sauvegarde sur un partage CIFS ou NFS.
   - **vFlash** pour enregistrer le fichier image de sauvegarde sur la carte vFlash.
3. Saisissez le nom du fichier de sauvegarde et la phrase de passe de chiffrement (facultatif).
4. Si **Réseau** est sélectionné comme emplacement du fichier, saisissez les paramètres de réseau.

REMARQUE : Lorsque vous indiquez les paramètres de partage du réseau, il est conseillé d'éviter l'utilisation des caractères spéciaux dans le nom d'utilisateur et mot de passe ou de crypter en pourcentage les caractères spéciaux.

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

5. Cliquez sur **Sauvegarder maintenant**.
   L'opération de sauvegarde est initialisée et vous pouvez afficher l'état sur la page **File d'attente des tâches**. Après une opération réussie, le fichier de sauvegarde est créée dans l'emplacement spécifié.

Sauvegarde du profil du serveur à l'aide de RACADM

Pour sauvegarder le profil du serveur à l'aide de RACADM, utilisez la commande `systemconfig backup`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Planification de la sauvegarde automatique du profil de serveur

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

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

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

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

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

Pour planifier la sauvegarde automatique du profil de serveur :

1. Dans l'interface Web d'iDRAC, allez à **Présentation** > **Paramètres iDRAC** > **Profil du serveur**.
   La page **Sauvegarde et exportation du profil du serveur** s'affiche.
2. Cliquez sur l'onglet de **sauvegarde automatique**.
3. Sélectionnez l'option **Activer la sauvegarde automatique**.
4. Sélectionnez un des éléments suivants pour enregistrer l'image du fichier de sauvegarde :
   - **Réseau** pour enregistrer l'image du fichier de sauvegarde sur un partage CIFS ou NFS.
     REMARQUE : CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.
   - **vFlash** pour enregistrer le fichier image de sauvegarde sur la carte vFlash.
5. Saisissez le nom du fichier de sauvegarde et la phrase de passe de chiffrement (facultatif).
6. Si **Réseau** est sélectionné comme emplacement du fichier, saisissez les paramètres de réseau.

   REMARQUE : Lorsque vous indiquez les paramètres de partage du 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 d'iDRAC*.
7. Dans la section **Calendrier de la fenêtre de sauvegarde**, spécifiez l'heure de début de l'opération de sauvegarde et la fréquence de l'opération (tous les jours, toutes les semaines ou tous les mois).

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
8. Cliquez sur **Planifier une sauvegarde**.

   Une tâche récurrente est présente dans la liste d'attente de tâches avec la date et l'heure de début de la prochaine opération de sauvegarde planifiée. Cinq minutes après le début de la première instance des tâches récurrentes, la tâche de la prochaine période est créée. L'opération de sauvegarde du profil de serveur est exécutée à la date et à l'heure planifiées.

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

Pour activer la sauvegarde automatique, utilisez la commande suivante :

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

Pour planifier une opération de sauvegarde de profil de serveur :

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

Pour afficher le calendrier de sauvegarde actuel :

```
racadm systemconfig getbackupscheduler
```

Pour désactiver la sauvegarde automatique, utilisez la commande suivante :

```
racadm set LifeCycleController.lcattributes.autobackup Disabled
```

Pour effacer le calendrier de sauvegarde :

```
racadm systemconfig clearbackupscheduler
```

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Importation du profil du serveur

Vous pouvez utiliser le fichier image de sauvegarde pour importer ou restaurer la configuration et le micrologiciel sur le même serveur sans avoir à redémarrer ce dernier.

La fonction d'importation s'utilise sans licence.

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

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

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

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

```
Restore is already running
```

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

Easy Restore

REMARQUE : Easy Restore est disponible uniquement sur les serveurs PowerEdge de 13e génération qui disposent de la mémoire flash Easy Restore. Easy Restore n'est pas disponible sur PowerEdge R930.

Après remplacement de la carte mère sur votre serveur, Easy Restore vous permet de restaurer automatiquement les données suivantes :

- Numéro de service du système
- Données des licences
- Application de diagnostics UEFI
- Paramètres de configuration du système (BIOS, iDRAC et NIC)

Easy Restore utilise la mémoire flash Easy Restore pour sauvegarder les données. Lorsque vous remplacez la carte mère et l'alimentation sur le système, 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 l'application de diagnostics UEFI. Le second écran du BIOS vous invite à restaurer les paramètres de configuration du système. Si, dans le premier écran du BIOS, vous choisissez de ne pas restaurer les données et si vous ne définissez pas le numéro de service par une autre méthode, le premier écran du BIOS s'affiche à nouveau. Le second écran du BIOS ne s'affiche qu'une seule fois.

REMARQUE :

- Les paramètres des configurations du système sont sauvegardés uniquement lorsque la fonction CSIOR est activée. Assurez-vous que Lifecycle Controller et CSIOR sont activés.
- L'effacement du système n'efface pas les données à partir de la mémoire flash Easy Restore.
- Easy Restore ne sauvegarde pas d'autres données comme les images de micrologiciel, les données vFlash ou les données de cartes d'extension.

Tâches associées

Séquence des opérations de restauration , page 79

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

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

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

   REMARQUE : Lorsque vous indiquez les paramètres de partage du réseau, il est conseillé d'éviter l'utilisation des caractères spéciaux dans le nom d'utilisateur et mot de passe ou de crypter en pourcentage les caractères spéciaux.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
5. Sélectionnez l'une des options suivantes pour la **configuration des disques virtuels et des données du disque dur** :
   - **Conserver** : conserve les informations sur le niveau de RAID, le disque virtuel, les attributs de contrôleur et le disque dur dans le système et restaure l'état du système à un état antérieur à l'aide du fichier image de sauvegarde.
   - **Supprimer et remplacer** : supprime et remplace les informations sur le niveau de RAID, le disque virtuel, les attributs de contrôleur et la configuration du disque dur dans le système à l'aide des données du fichier image de sauvegarde.
6. Cliquez sur **Importer**.
   L'importation de profil de serveur est lancée.

Importation du profil du serveur à l'aide de RACADM

Pour importer le profil du serveur à l'aide de RACADM, utilisez la commande `systemconfig restore`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Séquence des opérations de restauration

La séquence des opérations de restauration est la suivante :

1. Le système hôte s'éteint.
2. Les informations des fichiers de sauvegarde sont utilisées pour restaurer le Lifecycle Controller.
3. Le système hôte s'allume.
4. Le processus de restauration du micrologiciel et de la configuration pour les périphériques est terminé.
5. Le système hôte s'éteint.

6. Le processus de restauration du micrologiciel iDRAC et de la configuration est terminé.
7. iDRAC redémarre.
8. Le système hôte restauré s'allume pour fonctionner à nouveau normalement.

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

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

4

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

Configurez iDRAC en utilisant :

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

Pour configurer iDRAC :

1. Connectez-vous à l'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 sériel sur LAN
   - IPMI sur le LAN
   - Client SSH ou Telnet
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. Configurez la carte vFlash, si nécessaire.
15. Définissez le premier périphériques de démarrage, si nécessaire.
16. Définissez la connexion directe entre le SE et iDRAC, le cas échéant.

Concepts associés

Ouverture de session dans iDRAC , page 30
Modification des paramètres réseau , page 82
Configuration des services , page 86
Configuration de l'écran du panneau avant , page 90
Définition de l'emplacement du système géré , page 52
Configuration du fuseau horaire et NTP , page 91
Configuration de la communication iDRAC , page 114
Configuration des comptes et des privilèges des utilisateurs , page 133
Surveillance et gestion de l'alimentation , page 178
Activation du dernier écran de blocage , page 93

Configuration et utilisation de la console virtuelle , page 238
Gestion de Média Virtuel , page 247
Gestion de la carte SD vFlash , page 257
Définition du premier périphérique de démarrage , page 92
Activation ou désactivation de la connexion directe entre le SE et l'iDRAC , page 93

Tâches associées

Configuration d'iDRAC pour envoyer des alertes , page 161

Sujets :

- Affichage des informations iDRAC
- Modification des paramètres réseau
- Sélection des suites de chiffrement
- Mode FIPS
- Configuration des services
- Utilisation du client VNC pour gérer le serveur distant
- Configuration de l'écran du panneau avant
- Configuration du fuseau horaire et NTP
- 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 d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Propriétés** pour afficher les informations suivantes associées à iDRAC. Pour plus d'informations sur les propriétés, voir l'*Aide en ligne d'iDRAC*.

- Version matérielle et du micrologiciel
- Dernière mise à jour du micrologiciel
- Heure RAC
- Version d'IPMI
- Informations de barre de titre de l'interface utilisateur
- Paramètres réseau
- Paramètres IPv4
- Paramètres IPv6

Affichage des informations iDRAC à l'aide de RACADM

Pour afficher les informations iDRAC à l'aide de RACADM, consultez les informations relatives aux sous-commandes `getsysinfo` ou `get` dans le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Modification des paramètres réseau

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

Pour pouvoir modifier les paramètres réseau 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 Web

Pour modifier les paramètres réseau iDRAC :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau**.
   La page **Réseau** s'affiche.
2. Spécifiez les paramètres réseau, paramètres communs, IPv4, IPv6, IPMI et/ou paramètres VLAN, selon vos besoins, puis cliquez sur **Appliquer**.

   Si vous sélectionnez **Carte réseau 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 le temps d'arrêt à l'aide de RACADM ou WSMAN.

   Pour plus d'informations sur les champs, voir l'*aide en ligne d'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 iDRAC est désactivé, même si DHCP est activé.

Configuration du filtrage IP

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

- Le filtrage IP limite la plage d'adresses IP des clients qui accèdent à iDRAC. Il compare l'adresse IP de la connexion entrante à la plage définie et permet l'accès à iDRAC uniquement depuis une station de gestion dont l'adresse IP se trouve dans la plage. Toutes les autres demandes de connexion sont rejetées.
- Lorsque plusieurs échecs de connexion se produisent depuis une adresse IP spécifique, cela empêche la connexion de l'adresse à iDRAC pendant une période prédéfinie. Après deux échecs de tentative de connexion, vous devez patienter 30 secondes avant de vous connecter de nouveau. Après plus de deux échecs de tentative de connexion, vous devez patienter 60 secondes avant de vous connecter de nouveau.

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

REMARQUE : Lorsque des tentatives de connexion sont refusées depuis l'adresse IP du client, certains clients SSH peuvent afficher le message suivant : `ssh exchange identification: Connection closed by remote host`.

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

Configurer le filtrage IP à l'aide de l'interface Web d'iDRAC

Vous devez détenir le privilège de configuration pour effectuer ces étapes.

Pour configurer le filtrage IP :

1. Dans l'interface Web d'iDRAC, allez sur **Présentation** > **Paramètres iDRAC** > **Réseau** > **Réseau**.
   La page **Réseau** s'affiche.
2. Cliquez sur **Paramètres avancés**.
   L'écran **Sécurité du réseau** s'affiche.
3. Spécifiez les paramètres de filtrage IP.
   Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC*.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration du filtrage des IP à l'aide de RACADM

Vous devez détenir le privilège de configuration pour effectuer ces étapes.

Pour configurer le filtrage des IP, utilisez les objets RACADM suivants dans le groupe `iDRAC.IPBlocking` :

- RangeEnable
- RangeAddr
- RangeMask

La propriété `RangeMask` est appliquée à l'adresse IP entrante et à la propriété `RangeAddr`. Si les résultats sont identiques, la demande de connexion entrante est autorisée à accéder à l'iDRAC. La connexion à partir d'adresses IP hors de cette plage génère une erreur.

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

```
RangeMask & (<incoming-IP-address> ^ RangeAddr)
```

&
: Opérateur de bits AND des quantités

^
: Opérateur de bits OR exclusif

Exemples pour le filtrage IP

Les commandes RACADM suivantes bloquent toutes les adresses IP, sauf l'adresse 192.168.0.57 :

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

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

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

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

Pour en savoir plus, voir l'*iDRAC RACADM Command Line Reference Guide* (Guide de référence de ligne de commande RACADM iDRAC) disponible à l'adresse **dell.com/idracmanuals**.

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 iDRAC, ou encore les interfaces de ligne de commande RACADM et WSMan.

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

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

PRÉCAUTION : 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 vérifier et valider la configuration de la suite de chiffrement qui en résulte, afin de vous assurer que les résultats s'alignent sur les attentes et les exigences.**

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

Pour ajouter des chaînes chiffrées personnalisées :

1. Dans l'interface web d'iDRAC, allez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Service** pour accéder au paramètres du 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**, entrez une chaîne valide et sélectionnez **Définir une chaîne chiffrée**.

   REMARQUE : Pour obtenir la liste des chaînes chiffrées, voir www.openssl.org/docs/man1.0.2/apps/ciphers.html.

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.

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 iDRAC*, disponible sur **dell.com/idracmanuals**.

Mode FIPS

FIPS est une norme de sécurité informatique que doivent utiliser les agences et les sous-traitants du gouvernement des États-Unis. À partir de sa version 2.40.40.40, 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

Les logiciels qui ont été validés par l'exécution du programme de validation du module cryptographique sont désignés comme FIPS validé. Compte tenu du temps nécessaire pour effectuer la validation FIPS, les versions d'iDRAC ne sont pas toutes validées. Pour plus d'informations sur le statut à jour de la validation FIPS pour iDRAC, reportez-vous à la page du programme de validation du module cryptographique sur le site web NIST.

Activation du mode FIPS

PRÉCAUTION : L'activation du mode FIPS réinitialise iDRAC en le ramenant à ses paramètres d'usine par défaut. Si vous souhaitez restaurer les paramètres, sauvegardez le profil de configuration du serveur (SCP) avant d'activer le mode FIPS et restaurez le SCP après le redémarrage d'iDRAC.

REMARQUE : Si vous réinstallez ou mettez à niveau le micrologiciel iDRAC, le mode FIPS est désactivé.

Activation du mode FIPS à l'aide de l'interface web

1. Dans l'interface web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau**.
2. Cliquez sur **Paramètres avancés** en regard de **Options**.
3. En **mode FIPS**, sélectionnez **Activé** et cliquez sur **Appliquer**.
4. Un message apparaît vous invitant à confirmer la modification. Cliquez sur **OK**.
   L'iDRAC redémarre en mode FIPS. Attendez au moins 60 secondes avant de vous reconnectez-vous à l'iDRAC.
5. Installez un certificat de confiance pour l'iDRAC.

   REMARQUE : Le certificat SSL par défaut n'est autorisé qu'en mode FIPS.

REMARQUE : Certaines interfaces iDRAC, comme les implémentations d'IPMI et de SNMP conformes aux standards, ne prennent pas en charge la conformité FIPS.

Activation du mode FIPS à l'aide de RACADM

Utilisez la CLI RACADM pour exécuter la commande suivante :

```
racadm set iDRAC.Security.FIPSMode <Enable>
```

Désactivation du mode FIPS

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

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.
web Server	Activez l'accès à l'interface web d'iDRAC. Si vous désactivez l'interface web, l'interface RACADM distante est également désactivée. Utilisez l'interface RACADM locale pour réactiver le serveur web et la RACADM distante.
SSH	Accédez à iDRAC via le micrologiciel de RACADM.
Telnet	Accédez à iDRAC via le micrologiciel de RACADM.
Interface RACADM distante	Accédez à distance à iDRAC.

Redfish	Active la prise en charge de l'API RESTful Redfish.
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.
Serveur VNC	Activez le serveur VNC avec ou sans chiffrement SSL.

Configuration des services en utilisant l'interface web

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

1. Dans l'interface web iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **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.

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.Telnet
- iDRAC.Racadm
- iDRAC.SNMP

Pour plus d'informations sur ces objets, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Activation ou désactivation de la redirection HTTPs

Si vous ne souhaitez pas de redirection automatique de HTTP à HTTPs en raison d'un avertissement concernant le certificat iDRAC par défaut ou en tant que paramètre temporaire de débogage, vous pouvez configurer l'iDRAC de sorte que la redirection de port http (la valeur par défaut est 80) vers le port https (la valeur par défaut est 443) est désactivée. Par défaut, elle est activée et vous devez vous déconnecter, puis vous reconnecter à l'iDRAC pour que ce paramètre prenne effet. Lorsque vous désactivez cette fonction, un message d'avertissement s'affiche.

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

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

Pour désactiver le protocole HTTP à HTTPs pour la redirection :

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

Pour activer le protocole HTTP à HTTPs pour la redirection :

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

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

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

Configuration de TLS

Par défaut, l'iDRAC est configuré pour utiliser TLS 1.1 et plus récent. Vous pouvez le configurer pour qu'il utilise l'une des versions suivantes :

- TLS 1.0 et plus récent
- TLS 1.1 et plus récent
- TLS 1.2 uniquement

REMARQUE : Pour assurer une connexion sécurisée, Dell recommande d'utiliser TLS 1.1 et plus récent.

Configuration de TLS à l'aide de l'interface web

1. Allez dans **Présentation** > **Paramètres iDRAC** > **Réseau**.
2. Cliquez sur l'onglet **Services**, puis sur **Serveur web**.
3. Dans la liste déroulante **Protocole TLS**, sélectionnez la version de TLS et cliquez sur **Appliquer**.

Configuration de TLS à l'aide de RACADM

Pour vérifier la version de TLS configurée :

```
racadm get idrac.webserver.tlsprotocol
```

Pour définir la version de TLS :

```
racadm set idrac.webserver.tlsprotocol <n>
```

<n>=0
: TLS 1.0 et versions ultérieures

<n>=1
: TLS 1.1 et versions ultérieures

<n>=2
: TLS 1.2 uniquement

Utilisation du client VNC pour gérer le serveur distant

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

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

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

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

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

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

REMARQUE :

- Lorsque la carte NIC iDRAC est en mode partagé et le système hôte est hors tension puis de nouveau sous tension, 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 l'expiration du délai d'attente (la valeur configurée dans les paramètres du serveur VNC dans la page **Services** de l'interface web 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 iDRAC

Pour configurer les paramètres de serveur VNC :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Services**.
   La page **Services** s'affiche.
2. Dans la section **Serveur VNC**, activez le serveur VNC, spécifiez le mot de passe, le numéro de port et l'activation ou la désactivation du cryptage SSL.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne 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 en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration de VNC Viewer avec cryptage SSL

Lors de la configuration des paramètres du serveur VNC dans l'iDRAC, si l'option **Cryptage SSL** a été activé, l'application de tunnel SSL doit être utilisée avec le VNC Viewer pour établir la connexion SSL crypté 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 qu'il accepte la connexion sur `<localhost>:<localport number>`. Par exemple, 127.0.0.1:5930.
2. Configurez le tunnel SSL pour qu'il se connecte 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 général, tous les VNC Viewers à distance conformes RFB (Remote Frame Buffer) se connectent au serveur VNC à l'aide de l'adresse IP d'iDRAC et du numéro de port configuré pour le serveur VNC. Si l'option de cryptage SSL est désactivée lors de la configuration des paramètres du serveur VNC dans l'iDRAC, pour vous connecter au VNC Viewer effectuez les opérations suivantes :

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 `<iDRAC IP address:VNC port number>`

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

Configuration de l'écran du panneau avant

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

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

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

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

Concepts associés

Configuration du paramétrage LCD , page 90
Configuration du paramétrage LED d'ID système , page 91

Configuration du paramétrage LCD

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

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

Pour configurer l'écran LCD du panneau avant :

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

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

     Si vous sélectionnez **Aucun**, le message d'accueil ne s'affiche pas sur l'écran LCD du panneau avant du serveur.
3. Activer l'indication de la console virtuelle (facultatif). Si cette indication est activée, la section Alimentation du panneau avant actuelle et l'écran LCD du serveur affichent le message `Session de la console virtuelle active` lorsqu'une session de la console virtuelle est active.
4. Cliquez sur **Appliquer**.
   L'écran LCD affiche le message d'accueil défini.

Définition des paramètres LCD en utilisant RACADM

Pour configurer l'écran LCD du panneau avant, utilisez les objets du groupe `System.LCD`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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

Pour configurer l'écran LCD du panneau avant :

1. Dans l'utilitaire Paramètres iDRAC, allez sous **Sécurité du panneau avant**.
   La page **Sécurité du panneau avant des paramètres iDRAC** s'affiche
2. Activez ou désactivez le bouton d'alimentation.
3. Paramétrez les options suivantes :
   - Accès au panneau avant
   - Chaîne de messages LCD
   - Unités d'alimentation du système, unités de température ambiante, et affichage d'erreurs
4. Activez ou désactivez l'indication de la console virtuelle.
   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
5. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

Configuration du paramétrage LED d'ID système

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

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

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

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Matériel** > **Panneau avant**. La page **Panneau avant** s'affiche.
2. Dans la section **Paramètres LED d'ID du système**, sélectionnez les options suivantes pour activer ou désactiver le clignotement LED :
   - clignotement désactivé
   - clignotement activé
   - clignotement activé pour un jour
   - clignotement activé pour une semaine
   - clignotement activé pour un mois
3. Cliquez sur **Appliquer**.
   Le clignotement LED est configuré sur le panneau avant.

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

Pour configurer le voyant LED d’identification du système, utilisez la commande `setled`.

Pour en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration du fuseau horaire et NTP

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

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

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

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

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

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

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

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 premier périphérique de démarrage

Vous pouvez définir le premier périphérique de démarrage soit uniquement pour le démarrage suivant, soit pour tous les démarrages ultérieurs. Si vous définissez le périphérique pour tous les démarrages ultérieurs, il restera le premier périphérique dans la séquence de démarrage du BIOS jusqu'à ce que vous en changiez à nouveau dans l'interface web d'iDRAC ou dans 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
- Carte SD locale
- vFlash
- Lifecycle Controller
- BIOS Boot Manager (Gestionnaire d'amorçage du BIOS)
- Chemin d'accès au périphérique UEFI

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.
- Utilisez l'interface Redfish pour définir le chemin d'accès au périphérique UEFI. L'amorçage sur le chemin d'accès à un périphérique UEFI est pris en charge sur les serveurs Dell de 13e génération ou plus récents.

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 **Présentation générale** > **Serveur** > **Installation** > **Périphérique de démarrage initial**.
   L'écran **Périphérique de démarrage initial** s'affiche.
2. Sélectionnez le premier périphérique de démarrage dans la liste déroulante et cliquez sur **Appliquer**.
   Le système démarre depuis le périphérique sélectionné pour les démarrages suivants.

3. Pour démarrer depuis le périphérique une seule fois lors du démarrage suivant, sélectionnez **Boot Once** (Démarrer une seul fois). Ensuite, le système démarre depuis le premier périphérique de démarrage dans la séquence de démarrage du BIOS.

   Pour plus d'informations sur les options, voir l'*Aide en ligne d'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 d'amorçage ponctuel pour un périphérique, utilisez l'objet `iDRAC.ServerBoot.BootOnce`.

Pour plus d'informations sur ces objets, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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

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

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

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

Activation du dernier écran de blocage

Pour identifier la cause d'un blocage du système géré, capturez l'image de ce blocage à l'aide d'iDRAC.

REMARQUE : Pour plus d'informations sur Server Administrator, consultez le *Guide d'installation de Dell OpenManage Server Administrator*, disponible sur **l'adresse dell.com/support/manuals**. Pour plus d'informations sur iSM, voir Utilisation de l'iDRAC Service Module , page 275.

1. À partir du DVD *Dell Systems Management Tools and Documentation* ou à partir du site web de support de Dell, installez Server Administrator ou iDRAC Service Module (iSM) sur le système géré.
2. Dans la fenêtre de démarrage et de récupération de **Windows**, vérifiez que l'option de redémarrage automatique n'est pas sélectionnée.

   Pour plus d'informations, voir la documentation de Windows.
3. Utilisez Server Administrator pour activer le minuteur de **récupération auto**, affectez à l'action de récupération automatique la valeur **Réinitialiser Mettre hors tension** ou **Cycle d'alimentation** et définissez les secondes pour le minuteur (valeur comprise entre 60 et 480).
4. Activez l'option **Arrêt et récupération automatiques** (ASR) en utilisant l'un des éléments suivants :
   - Server Administrator : consultez le *Guide d'utilisation de Dell OpenManage Server Administrator*.
   - Interface RACADM locale : utilisez la commande `racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1`
5. Activez l'**agent de récupération de système automatique**. Pour ce faire, accédez à **Présentation générale** > **Paramètres iDRAC** > **Services** > **Réseau**, sélectionnez **Activé** et cliquez sur **Appliquer**.

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

Dans les serveurs équipés d'une carte réseau fille (NDC) 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 (serveurs rack ou tour), d'une carte réseau dédiée (serveurs rack, tour ou lame) ou via la carte réseau USB. Cette fonction est disponible avec la licence iDRAC Enterprise.

REMARQUE : Le module de service iDRAC (iSM) offre davantage de fonctionnalités pour gérer iDRAC via le système d'exploitation. Pour en savoir plus, voir l'*iDRAC Service Module User's Guide* (Guide d'utilisation du module Service iDRAC) disponible à l'adresse **dell.com/support/manuals**.

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

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

Vous pouvez activer ce canal à l'aide de :

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

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 fonction 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 de la carte réseau 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 entre en conflit avec l'adresse IP d'autres interfaces du système hôte ou du réseau local, vous devez la modifier.

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 A/A.

Références connexes

Cartes prises en charge pour la connexion directe entre le système d'exploitation et l'iDRAC , page 94
Systèmes d'exploitation pris en charge pour la carte réseau USB , page 95
Activation ou désactivation de la connexion directe à l'iDRAC à l'aide de l'interface Web , page 97
Activation ou désactivation de la connexion directe entre l'OS et l'iDRAC à l'aide de RACADM , page 97
Activation ou désactivation de la connexion directe à l'iDRAC à l'aide de l'utilitaire de paramètres iDRAC , page 97

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

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

Tableau 11. Connexion directe entre le système d'exploitation et l'iDRAC en utilisant la fonction LOM

Catégorie	Fabricant	Type
NDC	Broadcom	• 5720 QP rNDC 1 G BASE-T

Tableau 11. Connexion directe entre le système d'exploitation et l'iDRAC en utilisant la fonction LOM (suite)

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

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

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

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

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

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

- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2 (64 bits)
- Windows Server 2012
- Windows Server 2012 R2
- SUSE Linux Enterprise Server 10 SP4 (64 bits)
- SUSE Linux Enterprise Server 11 SP2 (64 bits)
- SUSE Linux Enterprise Server 11 SP4
- RHEL 5.9 (32 bits et 64 bits)
- RHEL 6.4
- RHEL 6.7
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U3
- vSphere v5.1 U1 ESXi
- vSphere v5.5 ESXi
- vSphere v5.5 U3
- vSphere 6.0
- VSphere 6.0 U1
- CentOS 6.5
- CentOS 7.0
- Ubuntu 14.04.1 LTS
- Ubuntu 12.04.04 LTS
- Debian 7.6 (Wheezy)
- Debian 8.0

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

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

Si le système d'exploitation de l'hôte est SUSE Linux Enterprise Server 11, CentOS 6.5, CentOS 7.0, Ubuntu 14.04.1 LTS ou Ubuntu 12.04.4 LTS, après l'activation de la carte réseau USB sur l'iDRAC, vous devez activer manuellement le client DHCP sur le système d'exploitation hôte. Pour plus d'informations sur l'activation de DHCP, voir la documentation relative aux systèmes d'exploitation SUSE Linux Enterprise Server, CentOS et Ubuntu.

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

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

Tableau 12. Informations relatives à la carte réseau USB sur les systèmes d'exploitation pris en charge

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

Sur le système hôte, lors de l'installation du système d'exploitation RHEL 5.9, le mode de connexion directe de la carte réseau USB est à l'état désactivé. S'il est activé à la fin de l'installation, l'interface réseau associée au dispositif de carte réseau USB n'est pas automatiquement activée. Vous pouvez activer le dispositif de carte réseau USB de différentes façons :

- Configurez l'interface de la carte réseau USB à l'aide de l'outil Network Manager. Sélectionnez **System (Système)** > **Administrator (Administrateur)** > **Network (Réseau)** > **Devices (Dispositifs)** > **New (Nouveau)** > **Ethernet Connection (Connexion Ethernet)** et sélectionnez **Dell computer corp.iDRAC Virtual NIC USB Device (Dispositif de carte réseau USB virtuelle iDRAC Dell)**. Cliquez sur l'icône Activate (Activer) pour activer le dispositif. Pour plus d'informations, voir la documentation RHEL 5.9.
- Créez le fichier de configuration de l'interface correspondante sous le nom `ifcfg-ethX` dans le répertoire `/etc/sysconfig/network-script/`. Ajoutez les entrées de base DEVICE, BOOTPROTO, HWADDR et ONBOOT. Ajoutez le TYPE dans le fichier `ifcfg-ethX` et redémarrez les services réseau en utilisant la commande `service network restart`.
- Redémarrez le système.
- Éteignez et mettez le système sous tension.

Sur les systèmes exécutant le système d'exploitation RHEL 5.9, si la carte réseau USB est désactivée et que vous arrêtez le système (ou vice versa), lors du redémarrage du système : si la carte réseau USB est activée, le dispositif de carte réseau USB n'est pas automatiquement activé. Pour l'activer, vérifiez si un fichier `ifcfg-ethX.bak` est disponible dans le répertoire `/etc/sysconfig/network-script` pour l'interface de carte réseau USB. S'il est disponible, renommez-le `ifcfg-ethX`, puis utilisez la commande `ifup ethX`

Tâches associées

Installation des fichiers VIB , page 96

Installation des fichiers VIB

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

Pour installer le fichier VIB :

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

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

   Le résultat est :

```
Message : The update completed successfully, but the system needs to be
rebooted for the changes to be effective. Reboot Required: true VIBs Installed:
Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03 VIBs Removed: VIBs Skipped:
```

3. Redémarrez le serveur.
4. À l'invite ESXi, exécutez la commande : `esxcfg-vmknic l`.

Le résultat affiche l'entrée usb0.

Activation ou désactivation de la connexion directe à l'iDRAC à l'aide de l'interface Web

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

1. Allez sous **Présentation** > **Paramètres iDRAC** > **Réseau** > **Connexion directe entre le SE et iDRAC**.
   La page **Connexion directe entre le SE et iDRAC** s'affiche.
2. Sélectionnez l'une des options suivantes pour activer la connextion directe entre le système d'exploitation et l'iDRAC :
   - **LOM** : le lien de transfert du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le périphérique LOM ou NDC.
   - **USB** : le lien de transfert du SE à l'iDRAC entre l'iDRAC et le système d'exploitation hôte est établi via le bus USB interne.

   Pour désactiver cette fonction sélectionnez **Désactivée**.
3. Si vous sélectionnez **LOM** en tant que configuration de transfert, et que le serveur est connecté à l'aide du mode dédié, saisissez l'adresse IPv4 du système d'exploitation.

   REMARQUE : Si le serveur est connecté en mode LOM partagé, le champ **Adresse IP du SE** est désactivé.
4. Si vous choisissez **Carte réseau USB** comme configuration de connexion directe, entrez l'adresse IP de la carte réseau USB.

   La valeur par défaut est 169.254.0.1. Il est conseillé d'utiliser l'adresse IP par défaut. Toutefois, 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.

   Ne saisissez pas les adresses IP 169.254.0.3 et 169.254.0.4. Ces adresses IP sont réservées pour la carte réseau USB à l'avant du panneau lorsqu'un câble A/A utilisé.
5. Cliquez sur **Appliquer** pour appliquer les paramètres.
6. Cliquez sur **Configuration réseau test** pour vérifier si l'IP est accessible et si le lien est établi entre l'iDRAC et le système d'exploitation hôte.

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

Pour activer ou désactiver la fonction Connexion directe entre l'OS et iDRAC à l'aide de RACADM, utilisez les objets du groupe `iDRAC.OS-BMC`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Activation ou désactivation de la connexion directe à l'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.

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

   La valeur par défaut est 169.254.0.1. Toutefois, si cette adresse IP entre en conflit avec une adresse IP d'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 pour le port NIC USB sur le panneau avant lorsqu'un câble A/A est utilisé.

5. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les informations sont enregistrées.

Obtention de certificats

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

Tableau 13. Types de certificats en fonction du type de connexion

Type de connexion	Type de certificat	Mode d'obtention
Connexion directe en utilisant Active Directory	Certificat CA de confiance	Générer un fichier RSC et le faire signer par une autorité de certification Les certificats SHA-2 sont également pris en charge.
Connexion avec une carte à puce comme utilisateur local ou Active Directory	• Certificat utilisateur • Certificat CA de confiance	• Certificat utilisateur : exportez le certificat utilisateur de carte à puce comme fichier codé en base 64 en utilisant le logiciel de gestion de carte fourni par le fournisseur de carte à puce. • Certificat CA de confiance : ce certificat est émis par une autorité de certification. Les certificats SHA-2 sont également pris en charge.
Connexion utilisateur Active Directory	Certificat CA de confiance	Ce certificat est émis par une autorité de certification. Les certificats SHA-2 sont également pris en charge.
Connexion d'utilisateur local	Certificat SSL	Générer un fichier RSC et le faire signer par une autorité de certification de confiance **REMARQUE :** iDRAC est équipé d'un certificat de serveur SSL auto-signé par défaut. Le serveur web iDRAC ainsi que les fonctions Virtual Media (média virtuel) et Virtual Console (console virtuelle) utilisent ce certificat. Les certificats SHA-2 sont également pris en charge.

Concepts associés

Certificats de serveur SSL , page 99
Génération d'une nouvelle demande de signature de certificat , page 100

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, 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 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.

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.

REMARQUE : Lors de l'accès à interface web iDRAC via FQDN, Mozilla Firefox peut ne pas reconnaître le certificat SSL comme étant digne de confiance. Pour continuer, ajoutez le certificat à la liste de confiance.

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.

Concepts associés

Génération d'une nouvelle demande de signature de certificat , page 100
Téléversement d'un certificat de serveur , page 100
Affichage du certificat de serveur , page 101
Téléversement d'un certificat de signature personnalisée , page 101
Télécharger un certificat de signature de certificat SSL personnalisé , page 102
Suppression d'un certificat de signature de certificat SSL personnalisé , page 102

Génération d'une nouvelle demande de signature de certificat

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

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

Lorsque l'autorité de certification accepte la demande CSR et émet le certificat de serveur SSL, ce dernier peut être téléversé vers iDRAC. Les informations utilisées pour générer la demande CSR, stockées dans le micrologiciel d'iDRAC, doivent correspondre aux informations contenues dans le certificat de serveur SSL, à savoir que le certificat doit avoir été généré en utilisant la demande CSR créée par iDRAC.

Concepts associés

Certificats de serveur SSL , page 99

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

Pour générer un fichier RSC :

REMARQUE : Chaque CSR remplace les données CSR stockées dans le micrologiciel. Les informations dans la CSR doivent correspondre aux informations dans le certificat de serveur SSL. Autrement, iDRAC n'accepte pas le certificat.

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **SSL**, sélectionnez **Générer une nouvelle demande de signature de certificat (CSR)** et cliquez sur **Suivant**.
   La page **Générer une nouvelle demande de signature de certificat** s'affiche.
2. Entrez une valeur pour chaque attribut RSC.
   Pour plus d'informations, voir l'*Aide en ligne d'iDRAC*.
3. Cliquez sur **Générer**.
   Un nouveau fichier CSR est généré. Enregistrez-le sur la station de gestion.

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 en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Téléversement d'un certificat de serveur

Après avoir généré un CSR, vous pouvez charger le certificat de serveur SSL vers le micrologiciel iDRAC. L'iDRAC doit être réinitialisé que le certificat soit appliqué. L'iDRAC accepte uniquement les certificats de serveur Web X509 codés en Base 64. Les certificats SHA-2 sont aussi pris en charge.

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

Concepts associés

Certificats de serveur SSL , page 99

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 iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **SSL**, sélectionnez **Téléverser un certificat de serveur** et cliquez sur **Suivant**.
   L'écran **Téléversement du certificat** s'affiche.
2. Sous **Chemin du fichier**, cliquez sur **Parcourir** et sélectionnez le certificat sur la station de gestion.

3. Cliquez sur **Appliquer**.
   Le certificat de serveur SSL est téléversé vers iDRAC.
4. Un message contextuel s'affiche vous demandant de réinitialiser l'iDRAC immédiatement ou à un moment ultérieur. Cliquez sur **Réinitialiser iDRAC** ou sur **Réinitialiser iDRAC** ultérieurement, au besoin.
   Après la réinitialisation d'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. Tant que l'iDRAC n'est pas réinitialisé, le certificat existant est actif.

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

Pour téléverser le certificat de serveur SSL, utilisez la commande `sslcertupload`. Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC* (Guide de référence de la ligne de commande RACADM d'iDRAC), disponible à l'adresse **dell.com/idracmanuals**.

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

1. Envoyez la RSC à une autorité de certification racine connue. L'autorité de certification signe la RSC, qui devient un certificat valide.
2. Téléversez la clé privée à l'aide de la commande racadm `sslkeyupload` à distance.
3. Téléversez le certificat signé sur l'iDRAC à l'aide de la commande racadm `sslcertupload` à distance.
   Le nouveau certificat est téléversé à l'iDRAC. Un message s'affiche vous demandant de réinitialiser l'iDRAC.
4. Exécutez la commande racadm `racreset` pour réinitialiser l'iDRAC.
   Après la réinitialisation d'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. Tant que l'iDRAC n'est pas réinitialisé, le certificat existant est actif.

Affichage du certificat de serveur

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

Concepts associés

Certificats de serveur SSL , page 99

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

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

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

Pour afficher le certificat de serveur SSL, utilisez la commande `sslcertview`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Téléversement d'un certificat de signature personnalisée

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

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

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

1. Allez dans **Présentation** > **Paramètres iDRAC** > **Réseau** > **SSL**.
   La page **SSL** s'affiche.
2. Sous **Certificat de signature de certificat SSL personnalisé**, sélectionnez **Téléverser le certificat de signature de certificat SSL personnalisé**, puis cliquez sur **Suivant**.
   La page **Téléverser le certificat de signature de certificat SSL personnalisé** s'affiche.
3. Cliquez sur **Parcourir** et sélectionnez le certificat de signature de certificat SSL personnalisé.

   Seul le certificat PKCS #12 (Public-Key Cryptography Standards #12 - Chiffrement de clé publique de norme n° 12) est pris en charge.
4. Si le certificat est protégé par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe du certificat PKCS#12**.
5. Cliquez sur **Appliquer**.
   Le certificat est téléversé vers iDRAC.
6. Un message contextuel s'affiche vous demandant de réinitialiser l'iDRAC immédiatement ou à un moment ultérieur. Cliquez sur **Réinitialiser iDRAC** ou sur **Réinitialiser iDRAC** ultérieurement, au besoin.
   Après la réinitialisation d'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. Tant que l'iDRAC n'est pas réinitialisé, le certificat existant est actif.

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

Pour téléverser le certificat de signature de certificat SSL personnalisé à l'aide de RACADM, utilisez la commande `sslcertupload`, puis utilisez la commande `racreset` pour réinitialiser l'iDRAC.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 du certificat de signature personnalisé

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

1. Allez dans **Présentation** > **Paramètres iDRAC** > **Réseau** > **SSL**.
   La page **SSL** s'affiche.
2. Sous **Certificat de signature de certificat SSL personnalisé**, sélectionnez **Télécharger le certificat de signature de certificat SSL personnalisé**, puis cliquez sur **Suivant**.
   Un message contextuel s'affiche vous permettant d'enregistrer le certificat de signature personnalisé sur un emplacement de votre choix.

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

Pour télécharger le certificat de signature de certificat SSL personnalisé, utilisez la sous-commande `sslcertdownload`. Pour en savoir plus, voir l'*iDRAC RACADM Command Line Interface Reference Guide* (Guide de référence de l'interface de ligne de commande RACADM DRAC) disponible à l'adresse **dell.com/idracmanuals**.

Suppression d'un certificat de signature de certificat SSL personnalisé

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

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

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

1. Allez dans **Présentation** > **Paramètres iDRAC** > **Réseau** > **SSL**.
   La page **SSL** s'affiche.
2. Sous **Certificat de signature de certificat SSL personnalisé**, sélectionnez **Supprimer le certificat de signature de certificat SSL personnalisé**, puis cliquez sur **Suivant**.
3. Un message contextuel s'affiche vous demandant de réinitialiser l'iDRAC immédiatement ou à un moment ultérieur. Cliquez sur **Réinitialiser iDRAC** ou sur **Réinitialiser iDRAC** ultérieurement, au besoin.
   Après la réinitialisation d'iDRAC, un nouveau certificat auto-signé est généré.

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

Pour supprimer à l'aide de RACADM le certificat de signature de certificat SSL personnalisé, utilisez la sous-commande `sslcertdelete`. Utilisez ensuite la commande `racreset` pour réinitialiser iDRAC.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration de plusieurs iDRAC à l'aide de RACADM

RACADM vous permet de configurer un ou plusieurs iDRAC avec des propriétés identiques. Lorsque vous interrogez un iDRAC en utilisant son ID de groupe et son ID d'objet, RACADM crée un fichier de configuration à partir des informations récupérées. Importez ce 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 pour configurer plusieurs iDRAC à l'aide de RACADM. Le fichier XML de configuration système contient les informations relatives à la configuration des composants. Vous pouvez utiliser ce fichier pour appliquer la configuration au BIOS, à l'iDRAC, au RAID et à la carte réseau en important le fichier dans un système cible. Pour en savoir plus, consultez le livre blanc *Flux de travail de la configuration XML*, disponible sur **dell.com/support/manuals** ou sur le Dell Tech Center.

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
   ```

   La commande demande la configuration iDRAC et génère le fichier de configuration.

   REMARQUE : La redirection d'une configuration iDRAC vers un fichier à l'aide de `get -f` n'est prise en charge qu'avec les interfaces RACADM 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. Le 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
   ```

La commande charge les informations vers 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 en utilisant la commande `racadm racreset`

Création d'un fichier de configuration iDRAC

Le fichier de configuration peut être :

- créé
- obtenu à l'aide de la commande `racadm get -f <file_name>.xml -t xml`
- Obtenu à l'aide de la commande `racadm get -f <file_name>.xml -t xml`, puis édité.

  Pour en savoir plus sur la commande `get`, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Le fichier de configuration est d'abord analysé pour vérifier que des noms de groupes et d'objets valides sont bien présents et que les règles de syntaxe de base sont respectées. Les erreurs sont indiquées avec le numéro de la ligne où l'erreur a été détectée, et un message explique le problème. La totalité du fichier est analysée pour vérifier qu'il est correct et toutes les erreurs sont affichées. Les commandes d'écriture ne sont pas transmises à iDRAC si une erreur est détectée dans le fichier. Vous devez corriger toutes les erreurs pour pouvoir utiliser le fichier afin de configurer iDRAC.

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

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 iDRAC via l'interface locale RACADM ou l'utilitaire de configuration d'iDRAC. Cependant, vous pouvez afficher ces paramètres de configuration. Pour ce faire :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Services**.
2. Sélectionnez l'une des options suivantes ou les deux :
   - **Désactiver la configuration local iDRAC à l'aide des paramètres iDRAC** — Désactive l'accès pour modifier les paramètres de configuration dans l'utilitaire de configuration iDRAC.
   - **Désactiver la configuration locale iDRAC à l'aide de l'interface RACADM** — Désactive l'accès pour modifier les paramètres de configuration dans l'interface locale RACADM.
3. Cliquez sur **Appliquer**.

   REMARQUE : Si l'accès est désactivé, vous ne pouvez pas utiliser Server Administrator ni IPMITool pour exécuter les configurations iDRAC. Cependant, vous pouvez utiliser IPMI sur le LAN.

5

Affichage des informations d'iDRAC et d'un système géré

Vous pouvez afficher l'intégrité et les propriétés d'iDRAC et d'un système géré, l'inventaire matériel et logiciel, l'intégrité des capteurs, les périphériques de stockage, les périphériques réseau et afficher les sessions utilisateur et y mettre fin. Pour les serveurs lames, vous pouvez également afficher les informations FlexAddress.

Concepts associés

Affichage de l'intégrité et des propriétés d'un système géré , page 105
Affichage de l'inventaire du système , page 106
Affichage des informations des capteurs , page 107
Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'E/S , page 108
Vérification de la conformité du système aux normes d'air frais , page 110
Affichage des données historiques de température , page 110
Inventaire et surveillance des périphériques de stockage , page 207
Inventaire et surveillance des périphériques réseau , page 184
Inventaire et surveillance des périphériques HBA FC , page 185
Visualisation des connexions de structure des cartes mezzanines FlexAddress , page 112
Affichage ou fin des sessions iDRAC , page 113

Sujets :

- Affichage de l'intégrité et des propriétés d'un système géré
- Affichage de l'inventaire du système
- Affichage des informations des capteurs
- Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'E/S
- Vérification de la conformité du système aux normes d'air frais
- Affichage des données historiques de température
- Affichage des interfaces réseau disponibles sur le SE hôte
- Visualisation des connexions de structure des cartes mezzanines FlexAddress
- Affichage ou fin des sessions iDRAC

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 du **Récapitulatif du système**, accédez à **Présentation** > **Serveur** > **Propriétés** > **Résumé**. La page **Récapitulatif du système** s'affiche. Pour en savoir plus, voir l'*aide en ligne d'iDRAC*.

Vous pouvez également afficher les informations de base du résumé du système en utilisant l'utilitaire de configuration d'iDRAC. Pour ce faire, dans l'utilitaire Paramètres iDRAC, accédez à **Résumé du système**. La page **Résumé du système - Paramètres d'iDRAC** s'affiche. Pour plus d'informations, voir l'*aide en ligne de l'utilitaire Paramètres iDRAC*.

Affichage de l'inventaire du système

Vous pouvez afficher des informations sur les composants matériel et micrologiciel installés sur le système géré. Pour ce faire, dans l'interface web iDRAC, accédez à **Présentation** > **Serveur** > **Propriétés** > **Inventaire système**. Pour plus d'informations sur les propriétés affichées, voir l'*aide en ligne d'iDRAC*.

La section Inventaire de matériel affiche les informations sur les composants suivants disponibles sur le système géré :

- iDRAC
- Contrôleur RAID
- Batteries
- UC
- Barrettes de mémoire DIMM
- Disque durs
- Fonds de panier
- Cartes d'interface réseau (incorporées et intégrées)
- Carte vidéo
- Carte SD
- Unité d'alimentation (PSU)
- Ventilateurs
- HBA Fibre Channel
- USB
- Périphériques SSD PCIe NVMe

La section Inventaire de micrologiel affiche la version de micrologiciel des composants suivants :

- BIOS
- Lifecycle Controller
- iDRAC
- Pack de pilotes du système d'exploitation
- Diagnostics 32 bits
- CPLD de système
- Contrôleurs PERC
- Batteries
- Disques physiques
- Alimentation
- NIC
- Fibre Channel
- Fond de panier
- Enceinte
- Cartes SSD PCIe

REMARQUE : L'inventaire des logiciels affiche uniquement les 4 derniers octets de la version du micrologiciel du composant. Par exemple, si la version du micrologiciel est FLVDL06, l'inventaire du micrologiciel affiche DL06.

REMARQUE : Sur les serveurs Dell PowerEdge FX2/FX2s, la convention d'affectation de noms de la version CMC affichée dans l'interface utilisateur graphique iDRAC est différente de celle affichée dans l'interface utilisateur graphique CMC. Toutefois, la version reste identique.

Lorsque vous remplacez un composant matériel ou mettez à jour les versions micrologicielles, veillez à activer et exécuter 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 informations des capteurs

Les capteurs suivant permettent de surveiller l'intégrité du système géré :

- **Batteries** : fournit des informations sur les batteries CMOS de la carte système et la carte ROMB (RAID On Motherboard) de stockage.

  REMARQUE : Les paramètres de la batterie ROMB de stockage sont disponibles uniquement si le système dispose d'une carte ROMB avec une batterie.
- **Ventilateur** (disponible uniquement pour les serveurs en rack et de type tour) : fournit des informations sur les ventilateurs du système (redondance de ventilateur et liste des ventilateurs qui indiquent la vitesse et les valeurs de seuil).
- **CPU (Processeur) :** indique l'intégrité et l'état des processeurs dans le système géré. Indique également la limitation automatique du processeur et les échecs prévisibles.
- **Mémoire** : affiche l'intégrité et l'état des barrettes de mémoire (DIMM) se trouvant sur le système géré.
- **Intrusion** : fournit des informations sur le châssis.
- **Blocs d'alimentation** (disponible uniquement sur les serveurs en rack et de type tour) : fournit des informations sur les blocs d'alimentation et l'état de redondance de ces blocs.

  REMARQUE : Si le système est doté d'un seul bloc d'alimentation, la redondance de bloc est **désactivée**.
- **Support flash amovible** : fournit des informations sur les modules SD internes : vFlash et module IDSDM (Internal Dual SD Module).
  - Lorsque la redondance IDSDM est activée, l'état du capteur IDSDM suivant est affiché : état de redondance IDSDM, IDSDM SD1, IDSDM SD2. Lorsque la redondance est désactivée, seul IDSDM SD1 est affiché.
  - Si la redondance IDSDM est désactivée initialement lorsque le système est mis sous tension ou après une réinitialisation d'iDRAC, l'état du capteur IDSDM SD1 est affiché uniquement après l'insertion d'une carte.
  - Si elle est activée avec deux cartes SD présentes dans le module IDSDM, et que l'état d'une carte SD est en ligne alors que celui de l'autre carte est hors ligne. Un redémarrage du système est nécessaire pour restaurer la redondance entre les deux cartes SD dans IDSDM. Une fois la redondance restaurée, l'état des deux cartes SD dans IDSDM est en ligne.
  - Au cours de l'opération de régénération pour restaurer la redondance entre les deux cartes SD présentes dans IDSDM, l'état IDSDM ne s'affiche pas, car les capteurs IDSDM sont hors tension.

    REMARQUE : Si le système hôte est redémarré pendant l'opération de reconstruction d'IDSDM, l'iDRAC n'affiche pas les informations IDSDM. Pour résoudre ce problème, reconstruisez de nouveau IDSDM ou réinitialisez l'iDRAC.

    REMARQUE : Sur les serveurs Dell PowerEdge de 13e génération, la reconstruction IDSDM est exécutée en arrière-plan et le système n'est pas arrêté durant le processus de reconstruction. Vous pouvez consulter l'état de l'opération de reconstruction dans les journaux Lifecycle Controller. Sur un serveur Dell PowerEdge de 12e génération, le système est arrêté durant l'exécution de l'opération de reconstruction.
  - Les journaux d'événements système (SEL) d'une carte protégée en écriture ou endommagée dans le module IDSDM ne sont pas répétés jusqu'à ce qu'ils soient effacés en remplaçant la carte SD par une carte SD inscriptible ou en bon état.
- **Temperature (Température)** : fournit des informations sur la température d'entrée et de sortie de la carte système (s'applique uniquement aux serveurs rack). La sonde de température indique si son état est entre les valeurs de seuil d'avertissement et de seuil critique prédéfinies.
- **Tension** : indique l'état et les valeurs des capteurs de tension des divers composants du système.

Le tableau suivant fournit des informations sur l'affichage des données des capteurs à l'aide de l'interface web iDRAC et de l'interface RACADM. Pour plus d'informations sur les propriétés affichées dans l'interface web, voir l'*Aide en ligne d'iDRAC*.

REMARQUE : La page Présentation du matériel affiche uniquement les données pour les capteurs présents sur votre système.

Tableau 14. Informations de capteurs à l'aide de l'interface web et de l'interface RACADM

Affichage des informations des capteurs	À l'aide de l'interface web	Utilisation de l'interface RACADM
Batteries	**Présentation** > **Matériel** > **Batteries**	Utilisez la commande `getsensorinfo`. Pour les blocs d'alimentations, vous pouvez également utiliser la commande `System.Power.Supply` avec la sous-commande `get`. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de*

Tableau 14. Informations de capteurs à l'aide de l'interface web et de l'interface RACADM (suite)

Affichage des informations des capteurs	À l'aide de l'interface web	Utilisation de l'interface RACADM
		commande RACADM iDRAC, disponible sur **dell.com/idracmanuals**.
Ventilateur	**Présentation** > **Matériel** > **Ventilateurs**	
Processeur	**Présentation** > **Matériel** > **UC**	
Mémoire	**Présentation** > **Matériel** > **Mémoire**	
Intrusion	**Présentation** > **Serveur** > **Intrusion**	
Blocs d'alimentation	**Présentation** > **Matériel** > **Blocs d'alimentation**	
Média flash amovible	**Présentation** > **Matériel** > **Média Flash amovible**	
Température	**Présentation** > **Serveur** > **Alimentation/ Thermique** > **Températures**	
	Présentation > **Serveur** > **Alimentation/ Thermique** > **Tensions**	

Surveillance de l'indice de performances du processeur, de la mémoire et des modules d'E/S

Sur les serveurs Dell PowerEdge de 13e génération, Intel ME prend en charge la fonctionnalité CUPS (Compute Usage Per Second). La fonction CUPS surveille en temps réel le processeur, la mémoire et l'utilisation des E/S, et fournit l'indice d'utilisation du système. Intel ME permet la surveillance des performances hors bande (OOB) et ne consomme pas les ressources du processeur. Intel ME comporte un capteur CUPS qui fournit les valeurs d'utilisation des ressources de calcul, de la mémoire et des E/S sous forme d'indice CUPS. IDRAC surveille cet indice CUPS pour obtenir le taux d'utilisation globale du système et surveille également l'indice d'utilisation instantanée du processeur, de la mémoire et des E/S.

REMARQUE : Cette fonctionnalité n'est pas prise en charge sur les serveurs PowerEdge R930.

Le processeur et le jeu de puces ont des compteurs de surveillance des ressources dédiés (RMC). Les données obtenues de ces RMC sont interrogées pour obtenir des informations sur l'utilisation des ressources système. Les données provenant de RMC sont agrégées par le gestionnaire de nœuds pour mesurer l'utilisation cumulée de chacune des ressources système qui sont lues à partir de l'iDRAC à l'aide de mécanismes d'intercommunication existants pour fournir des données via des interfaces de gestion hors bande.

La représentation du capteur Intel des valeurs d'indice et de paramètres de performances s'applique à l'ensemble du système physique. En conséquence de quoi, la représentation des données de performance sur les interfaces s'applique à l'ensemble du système physique, même si le système est virtualisé et héberge 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 :

- **CPU Utilization (Utilisation du processeur)** : les données de RMC pour chaque cœur de processeur sont agrégées pour fournir l'utilisation cumulée de tous les cœurs du système. Cette valeur est basée sur le temps passé à l'état actif et inactif. Un échantillon RMC est pris toutes les six secondes.
- **Memory Utilization (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 bande passante de la mémoire et non du taux d'utilisation de la mémoire. IDRAC l'agrège pendant une minute, de sorte qu'elle peut correspondre ou non à l'utilisation de la mémoire qu'affichent d'autres outils du SE, tels que **top** dans Linux. L'utilisation de la bande passante de mémoire que montre l'iDRAC indique si la charge de traitement consomme beaucoup de mémoire ou non.
- **I/O Utilization (Utilisation des E/S)** : il y a un RMC par port racine du Complexe racine PCI Express) pour mesurer le trafic PCI Express provenant ou dirigé vers ce port racine et le segment inférieur. Les données de ces RMC sont agrégées pour mesurer le trafic PCI Express de tous les segments PCI Express provenant du progiciel. Il s'agit de mesurer l'utilisation de la bande passante des E/S pour le système.

- **System Level CUPS Index (Indice CUPS au niveau système)** : l'indice CUPS est calculé en regroupant les indices du processeur, de la mémoire et des E/S, en prenant en compte un facteur de charge prédéfini de chaque ressource système. Le facteur de charge varie en fonction de la nature de la charge de travail sur le système. L'indice CUPS représente la mesure de la marge de calcul disponible sur le serveur. Si le système possède un fort indice CUPS, la marge pour ajouter des charges de travail sur ce système est limitée. Lorsque la consommation en ressources diminue, l'indice de CUPS du système diminue. Un faible indice CUPS indique que la marge de puissance de calcul est élevée, que le serveur peut recevoir de nouvelles charges de travail et qu'il fonctionne à puissance réduite pour limiter la consommation d'énergie. La surveillance de la charge de travail peut être appliquée dans tout le datacenter pour fournir une vue générale de haut niveau de la charge de travail du datacenter, ce qui en fait une solution dynamique pour ce dernier.

REMARQUE : Les indices d'utilisation du processeur, de la mémoire et des E/S sont agrégés sur une minute. Par conséquent, s'il existe des pics instantanés dans ces indices, ils peuvent être supprimés. Ils indiquent des types de charges de travail et non le taux d'utilisation des ressources.

Des interruptions IPMI, SEL et SNMP sont générées si les seuils des indices d'utilisation sont atteints et que les capteurs d'événements sont activés. Les indicateurs d'événements des capteurs sont désactivés par défaut. Ils peuvent être activés 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 performances du processeur, de la mémoire et des modules d'E/S via l'interface web

Pour surveiller l'indice de performances du processeur, de la mémoire et des modules d'E/S sur l'interface web de l'iDRAC, accédez à **Overview (Présentation)** > **Hardware (Matériel)**. La page **Hardware Overview (Présentation du matériel)** affiche les informations suivantes :

- Section **Matériel** : cliquez sur le lien voulu pour visualiser l'état du composant.
- 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 de l'UC, la mémoire, l'utilisation d'E/S et l'indice CUPS au niveau du système. Si le système hôte est hors tension, le graphique affiche la ligne hors tension en dessous de 0 %.
  - Vous pouvez réinitialiser l'utilisation maximale pour un capteur spécifique. Cliquez sur **Reset Historical Peak (Réinitialiser la valeur historique maximale)**. Pour réinitialiser la valeur maximale, vous devez disposer de privilèges de configuration.
- Section **Mesures de performances** :
  - Afficher l'état et la valeur actuelle.
  - Permet d'afficher ou de définir la limite d'utilisation du seuil d'avertissement. Vous devez disposer du privilège de configuration du serveur pour définir les valeurs de seuil.

REMARQUE : Les informations affichées sur cette page dépendent des capteurs pris en charge par le serveur. Les serveurs Dell PowerEdge de 12e génération et certains serveurs de 13e génération n'affichent pas les sections **System Performance (Performances du système)**, **System Performance Historical Data (Données historiques des performances du système)** et **Performance Metrics (Mesures de performances)**.

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

Surveillance de l'indice de performances du processeur, 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 en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Vérification de la conformité du système aux normes d'air frais

Le refroidissement à l'air frais utilise directement l'air extérieur pour refroidir les systèmes du centre de données. Les systèmes conformes aux normes d'air frais peuvent fonctionner au-dessus de leur plage de température ambiante de fonctionnement normale (températures jusqu'à 113 ° F (45 ° C)).

REMARQUE : Certains serveurs ou certaines configurations d'un serveur peuvent ne pas être conformes aux normes d'air frais. Reportez-vous au manuel du serveur spécifique relatif à la conformité aux normes d'air frais ou contactez Dell pour en savoir plus.

Pour vérifier la conformité du système aux normes d'air frais :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation / Thermique** > **Températures**.
   La page **Températures** s'affiche.
2. Reportez-vous à la section **Air frais** qui indique si le serveur est conforme ou non aux normes d'air frais.

Affichage des données historiques de température

Vous pouvez surveiller le pourcentage de temps pendant lequel le système a fonctionné à une température ambiante supérieure au seuil de température normalement toléré. La 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 stocker la température surveillée durant les sept dernières années.

REMARQUE : Vous pouvez suivre l'historique de la température, même pour les systèmes qui ne sont pas conformes aux normes d'air frais. Toutefois, les limites de seuil et les avertissements liés à l'air frais générés sont basés sur les limites d'air frais prises en charge. Les limites sont 42 °C pour un avertissement et 47 °C pour un seuil critique. Ces valeurs correspondent à des limites d'air frais de 40 °C et 45 °C avec une marge de 2 °C pour la précision.

Deux bandes de température fixes associées aux limites d'air frais sont suivies :

- Bande d'avertissement : temps pendant lequel 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 : temps pendant lequel 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 incrémente également le temps dans la bande d'avertissement.

Les données collectées sont représentées sous forme graphique pour suivre les niveaux de 10 % et 1 %. Les données de température enregistrées ne peuvent être effacées qu'avant l'expédition de l'usine.

Un événement est généré si le système continue de fonctionner à une température supérieure au seuil normalement pris en charge pour une période de fonctionnement précise. Si la température moyenne de la période de fonctionnement précise est supérieure 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 iDRAC pour générer des événements supplémentaires. Pour plus d'informations, reportez-vous à la section Setting alert recurrence event (Définition d'événement de récurrence d'alerte).

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 iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation / Thermique** > **Températures**.

La page **Températures** s'affiche.

2. Reportez-vous à la section **Données historiques de la température ambiante d'admission 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 d'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.

Affichage des données historiques de température à l'aide de l'interface RACADM

Pour afficher les données historiques à l'aide de l'interface RACADM, utilisez la commande `inlettemphistory`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration du seuil d'avertissement de température d'entrée

Vous pouvez modifier les valeurs de seuil d'avertissement minimale et maximale du capteur de température d'entrée du système. Si vous restaurez les valeurs par défaut, les seuils de température sont définis sur les valeurs par défaut. Vous devez avoir le privilège utilisateur pour définir les valeurs des seuils d'avertissement du capteur de température d'entrée.

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 iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation / Thermique** > **Températures**.
   La page **Températures** s'affiche.
2. Dans la section **Capteurs de température**, pour la **Température d'entrée de la carte système**, entrez les valeurs minimale et maximale du **Seuil d'avertissement** en degrés Celsius ou Fahrenheit. Si vous entrez la valeur en degrés Celsius, le système calcule automatiquement et affiche la valeur en degrés Fahrenheit. De même, si vous indiquez 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 prises en compte dans le graphique de données historiques car les limites du graphique indique uniquement les valeurs des limites d'air frais. Les avertissements de dépassement des seuils personnalisés sont différents des avertissements associés au dépassement des seuils d'air frais.

Affichage des interfaces réseau disponibles sur le SE hôte

Vous pouvez afficher des 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 d'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 de l'équipement réseau, le nom de l'interface réseau, sa description, son état, son type (Ethernet, tunnel, boucle de rappel, etc.), l'adresse de la passerelle, l'adresse du serveur DNS et l'adresse du serveur DHCP.

REMARQUE : Cette fonctionnalité est disponible sous les licences iDRAC Express et Enterprise.

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 **Présentation** > **Serveur** > **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 l'interface web

Pour afficher les interfaces réseau disponibles sur l'OS hôte à l'aide de l'interface web :

1. Accédez à **Présentation** > **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'équipement correspondant s'affiche dans la section **Hardware (Matériel)** > **Network Devices (Équipements réseau)**, dans laquelle vous pouvez afficher les informations sur l'équipement. Pour plus d'informations sur les propriétés, voir l'*Aide en ligne d'iDRAC*.
4. Cliquez sur l'icône ⊞ pour afficher plus d'informations.

   De même, la page **Hardware (Matériel)** > **Network Devices (Équipements réseau)**, permet d'afficher les informations sur l'interface réseau du système d'exploitation hôte associé à un équipement réseau. Cliquez sur **View Host OS Network Interfaces (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 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 *iDRAC RACADM Command Line Reference Guide (Guide de référence de la ligne de commande RACADM iDRAC)*, disponible sur **dell.com/idracmanuals**.

Visualisation des connexions de structure des cartes mezzanines FlexAddress

Dans les serveurs lames, FlexAddress permet d'utiliser des noms mondiaux et des adresses MAC (WWN/MAC) persistants assignés par le châssis pour chaque connexion de port de serveur géré.

Vous pouvez afficher les informations suivantes pour chaque port de carte Ethernet intégrée et mezzanine en option :

- Structures auxquelles les cartes sont connectées.
- Type de structure.
- Adresses MAC affectées par le serveur, par le châssis ou à distance.

Pour afficher les informations Flex Address dans iDRAC, configurez et activez la fonction Flex Address dans CMC (Chassis Management Controller). Pour en savoir plus, voir le *Dell Chassis Management Controller User Guide* (Guide d'utilisation Dell Chassis Management Controller) disponible sur le site **dell.com/support/manuals**. Les sessions de console virtuelle ou Média Virtuel existantes prennent fin si le paramètre FlexAddress est activé ou désactivé.

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

La fonction FlexAddress remplace les adresses MAC affectées par le serveur par des adresses MAC affectées par le châssis et elle est mise en œuvre pour iDRAC avec les LOM de lame, les cartes mezzanines et les module d'E/S. La fonction iDRAC FlexAddress prend en charge la conservation des adresses MAC de logement pour les iDRAC dans un châssis. L'adresse MAC affectée par le châssis est stockée dans la mémoire non volatile CMC et elle est envoyée à iDRAC pendant son démarrage ou lorsque CMC FlexAddress est activé.

Si CMC permet d'utiliser des adresses MAC affectées par le châssis, iDRAC affiche l'**adresse MAC** dans les pages suivantes :

- **Présentation** > **Serveur** > **Propriétés Détails** > **Informations iDRAC**.
- **Présentation** > **Serveur** > **Propriétés WWN/MAC**.
- **Présentation** > **Paramètres iDRAC** > **PropriétésInformations iDRAC** > **Paramètres réseau actuels**.
- **Présentation** > **Paramètres iDRAC** > **Réseau** > **Paramètres réseau**.

PRÉCAUTION : Lorsque FlexAddress est activé, si vous passez d'une adresse MAC affectée par le serveur à une adresse MAC attribuée par le châssis et vice–versa, l'adresse IP iDRAC change également.

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 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 d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Sessions**.
   La page **Sessions** affiche l'ID de session, le nom d'utilisateur, l'adresse IP et le type de session. Pour plus d'informations sur ces propriétés, voir l'*aide en ligne d'iDRAC*.
2. Pour mettre fin à la session, dans la colonne **Annuler**, cliquez sur l'icône de corbeille pour la session.

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 en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

6

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
- Services à distance

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 15. Modes de communication — Résumé

Mode de communication	Protocole pris en charge	Commandes prises en charge	Prérequis
Interface web iDRAC	Protocole Internet (https)	S/O	Serveur Web
Série en utilisant un câble Null modem DB9	Protocole série	RACADM SMCLP IPMI	Partie du micrologiciel d'iDRAC RAC Série ou IPMI Série sont activés
IPMI série sur LAN	Protocole IPMB (Intelligent Platform Management Bus) SSH Telnet	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
SMCLP	SSH Telnet	SMCLP	SSH ou Telnet sur iDRAC est activé
Interface RACADM distante	HTTPS	Interface RACADM distante	L'interface distance RACADM est installée et activée
Micrologiciel RACADM	SSH Telnet	Micrologiciel RACADM	Le micrologiciel RACADM est installé et activé.
Interface RACADM locale	IPMI	Interface RACADM locale	L'interface RACADM locale est installée
Services distants [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM est installé (Windows) ou OpenWSMAN est installé (Linux)
	Redfish	Divers plug-in de navigateur, CURL (Windows et Linux), demande Python, et modules JSON	Des Plug-in, CURL, les modules Python sont installés

Tableau 15. Modes de communication — Résumé (suite)

Mode de communication	Protocole pris en charge	Commandes prises en charge	Prérequis
[1] Pour plus d'informations, voir le *Lifecycle Controller Remote Services User's Guide* **(Guide d'utilisation des services à distance Lifecycle Controller)** disponible à l'adresse **dell.com/idracmanuals**.			

Concepts associés

Communication avec l'iDRAC via une connexion série à l'aide d'un câble DB9 , page 115
Permutation entre RAC Série et la console série à l'aide d'un câble DB9 , page 118
Communication avec l'iDRAC à l'aide de SOL IPMI , page 119
Communication avec l'iDRAC à l'aide d'IPMI sur LAN , page 124
Activation ou désactivation de l'interface distante RACADM , page 125
Désactivation de l'interface locale RACADM , page 126
Activation d'IPMI sur un système géré , page 126
Configuration de Linux pour la console série pendant le démarrage , page 126
Schémas cryptographiques SSH pris en charge , page 129

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
- Activation d'IPMI sur un système géré
- Configuration de Linux pour la console série pendant le démarrage
- Schémas cryptographiques SSH pris en charge

Communication avec 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
- IPMI série — Mode de base de connexion directe et mode terminal de connexion directe

REMARQUE : Dans le cas de serveurs lames, la connexion série est établie via le châssis. Pour plus d'informations, voir le *Guide d'utilisation du Chassis Management Controller*, disponible sur **dell.com/support/manuals**.

Pour établir la connexion série :

1. Configurez le BIOS pour activer la connexion série.
2. Connectez le câble Null Modem DB9 du port série de la station de gestion au connecteur série externe du système géré.
3. Vérifiez que le logiciel d'émulation de terminal de la station de gestion est configuré pour la connexion série en utilisant l'un des éléments suivants :
   - Linux Minicom dans un Xterm
   - HyperTerminal Private Edition (version 6.3) de Hilgraeve

   Selon le point en cours du processus de démarrage du système géré, vous pouvez voir l'écran du POST ou celui du système d'exploitation. Ceci dépend de la configuration : SAC pour Windows et des écrans du mode texte Linux pour Linux.
4. Activez les connexions RAC série ou IPMI série dans iDRAC.

Concepts associés

Configuration du BIOS pour une connexion série , page 116
Activation d'une connexion série RAC , page 116

Activation des modes de base et terminal de connexion série IPMI , page 116

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 **System BIOS Settings** > **Serial Communication** (Paramètres du BIOS du système, Communication série).
4. Sélectionnez **External Serial Connector** to **Remote Access device** (Connecteur série externe vers périphérique d'accès à distance).
5. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
6. Appuyez sur Échap pour quitter la **configuration du système**.

Activation d'une connexion série RAC

Après avoir configuré la connexion série dans le BIOS, activez RAC série dans 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 l'interface Web

Pour activer la connexion RAC série :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **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 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 des modes de base et terminal de connexion série IPMI

Pour activer l'acheminement 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 au programme, telle que IPMI shell (ipmish) qui est inclus dans BMU (Baseboard Management Utility). Par exemple, pour imprimer le journal des événements système en utilisant ipmish via le mode de base IPMI, exécutez la commande suivante :

  ```
  ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
  ```

- Mode terminal IPMI : prend en charge les commandes ASCII envoyées depuis un terminal série. Ce mode prend en charge un nombre limité de commandes (y compris le contrôle de l'alimentation) et de commandes IPMI brutes tapées sous forme de caractères hexadécimaux. Il permet d'afficher les séquences de démarrage du système d'exploitation jusqu'au BIOS lorsque vous ouvrez une session dans iDRAC via SSH ou Telnet.

Concepts associés

Configuration du BIOS pour une connexion série , page 116
Autres paramètres pour le mode Terminal série IPMI , page 117

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 d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Série**.
2. Sous **IPMI sériel**, spécifiez les valeurs des attributs. Pour plus d'informations sur les options, voir l'*Aide en ligne d'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, 38400, 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 à distance dans le programme de configuration du BIOS pour configurer le BIOS pour la connexion série.

Pour plus d'informations sur ces propriétés, voir la spécification IPMI 2.0.

Autres paramètres pour le mode Terminal série IPMI

Cette section fournit des informations sur les paramètres de configuration du mode Terminal série IPMI.

Définition d'autres paramètres pour le mode Terminal IPMI série à l'aide de l'interface Web

Pour définir les paramètres du mode Terminal série :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Série**
   La page **Serial** (Série) s'affiche.
2. Activez l'option IPMI serial (Série IMPI).
3. Cliquez sur **Paramètres du mode terminal.**
   La page **Paramètres du mode terminal** s'affiche.
4. Définissez les 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 à distance dans le programme de configuration du BIOS pour configurer le BIOS pour la connexion série.

Définition de paramètres supplémentaires pour le mode Terminal IPMI série à láide de RACADM

Pour configurer les paramètres du mode terminal, utilisez la commande `set` avec les objets du groupe `idrac.ipmiserial`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 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 le RAC est défini en mode série RAC) ou en mode connexion série dans lequel les commandes de terminal peuvent être émises si iDRAC est défini en mode terminal de connexion directe série IPMI.

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.

Communication avec l'iDRAC à l'aide de SOL IPMI

SOL (Serial Over LAN) IPMI 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. Avec SOL, vous pouvez :

- accéder à distance aux systèmes d'exploitation sans expiration de délai d'attente ;
- diagnostiquer des systèmes hôtes sur Emergency Management Services (EMS) ou Special Administrator Console (SAC) pour Windows ou dans un environnement Linux ;
- afficher l'avancement d'un serveur au cours du POST et reconfigurer le programme de configuration du BIOS.

Pour définir le mode de communication SOL :

1. Configurez le BIOS pour une connexion série.
2. Configurez iDRAC pour utiliser SOL.
3. Activez un protocole pris en charge (SSH, Telnet, IPMItool).

Concepts associés

Configuration du BIOS pour une connexion série , page 119
Configuration d'iDRAC pour utiliser SOL , page 119
Activation du protocole pris en charge , page 120

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 **System BIOS Settings** > **Serial Communication** (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. Ensuite, l'écran redirigé s'affiche correctement.

   REMARQUE : Si le chargeur de démarrage ou le système d'exploitation fournissent la redirection série (comme GRUB ou Linux), le paramètre **Redirection après démarrage** du BIOS doit être désactivé, cela afin d'éviter d'éventuels états de concurrence de plusieurs composants cherchant à 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 l'interface Web iDRAC

Pour configurer IPMI sur le LAN (SOL) :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Communication série sur le LAN**.
   L'écran **Communications série sur le LAN** apparaît.
2. Activez SOL, définissez les valeurs et cliquez sur **Appliquer**.
   Les paramètres SOL IPMI sont définis.
3. Pour définir la fréquence d'accumulation de caractères et le seuil d'envoi de caractères, sélectionnez **Paramètres avancés.**
   L'écran **Paramètres avancés Communication série sur LAN** s'affiche.
4. Définissez les valeurs des attributs et cliquez sur **Appliquer**.

   Les paramètres avancés SOL IPMI sont définis. Ces valeurs améliorent les performances.

   Pour plus d'informations sur les options, voir l'*Aide en ligne 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 : Le niveau de privilèges SOL IPMI minimal détermine le privilège minimal pour l'activation de la fonctionnalité 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, 38400, 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.

Activation du protocole pris en charge

Les protocoles pris en charge sont IPMI, SSH et Telnet.

Activation d'un protocole pris en charge à l'aide de l'interface Web

Pour activer SSH ou Telnet, accédez à **Présentation générale** > **Paramètres iDRAC** > **Réseau** > **Services** et sélectionnez **Activé** pour SSH ou Telnet.

Pour activer IPMI, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** et sélectionnez **Activer IPMI sur le LAN**. Vérifiez que la valeur **Clé de cryptage** correspond à des zéros ou appuyez sur la touche Retour arrière pour remplacer la valeur par des caractères NULL.

Activation d'un protocole compatible à l'aide de RACADM

Pour activer SSH ou Telnet, utilisez les commandes suivantes.

- Telnet

```
racadm set iDRAC.Telnet.Enable 1
```

- SSH

```
racadm set iDRAC.SSH.Enable 1
```

  Pour modifier le port SSH

```
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 ou Telnet

Tâches associées

SOL utilisant le protocole IPMI , page 121
SOL utilisant le protocole SSH ou Telnet , page 122

SOL utilisant le protocole IPMI

L'utilitaire SOL basé sur IPMI et IPMItool utilise RMCP+ fourni en utilisant des datagrammes UDP vers le port 623. RMCP+ améliore l'authentification, la vérification de l'intégrité des données et le chiffrement et permet de transporter plusieurs types de charges utiles en utilisant IPMI 2.0. Pour en savoir plus, 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+ à iDRAC doit être cryptée en utilisant la clé de cryptage (Key Generator (KG)Key). Vous pouvez définir la clé de cryptage à l'aide de l'interface web d'iDRAC ou l'utilitaire de Configuration d'iDRAC.

Pour démarrer une session SOL en utilisant IPMItool depuis une station de gestion :

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente SOL par défaut dans **Présentation** > **Paramètres iDRAC** > **Réseau** > **Services**.

1. Installez IPMITool depuis le DVD *Dell Systems Management Tools and Documentation*.

   Pour les instructions d'installation, voir le *Guide d'installation rapide du logiciel*.
2. 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 depuis IPMItool, appuyez sur ~, puis sur la touche 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.

SOL utilisant le protocole SSH ou Telnet

SSH (Secure Shell) et Telnet sont des protocoles réseau qui permettent d'exécuter des communications avec l'iDRAC via la ligne de commande. Vous pouvez analyser les commandes de l'interface distante RACADM et SMCLP via l'une ou l'autre de ces interfaces.

Pour renforcer la sécurité, l'option « authentification interactive par clavier » a été activée sur le serveur SSH iDRAC. Avec cette option, la plupart des clients SSH informent l'utilisateur par différentes invites, en anticipant les demandes potentielles du serveur SSH. Ces invites sont opportunistes, c'est-à-dire que les clients SSH ne savent pas si une boîte de dialogue d'authentification supplémentaire sera demandée par le serveur. Ainsi, lorsque ces invites sont vues, leur contexte et leur applicabilité doivent être compris et ignorés si nécessaire. Ce comportement est une caractéristique de la plupart des clients SSH qui prennent en charge l'option « authentification interactive par clavier » en plus des procédures normales « d'authentification par mot de passe » et « d'authentification par clé publique ». En outre, les libellés des « invites de boîte de dialogue » varient en fonction des différentes implémentations du client SSH.

SSH est plus sécurisé que Telnet. IDRAC prend uniquement en charge la version SSH 2, avec l'authentification par mot de passe, qui est activée par défaut. L'iDRAC prend en charge jusqu'à deux sessions SSH et deux sessions Telnet à la fois. Il est recommandé d'utiliser SSH, car Telnet n'est pas un protocole sécurisé. Vous devez utiliser Telnet uniquement si vous ne pouvez pas installer un client SSH ou si votre infrastructure réseau est sécurisée.

REMARQUE : Lors de l'établissement d'une connexion SSH, un message de sécurité s'affiche (« authentification supplémentaire requise »), car l'iDRAC prend désormais en charge « l'authentification interactive par clavier» pour une sécurité renforcée.

Utilisez des programmes Open Source, tels que PuTTY ou OpenSSH, qui prennent en charge les protocoles de réseau SSH et Telnet sur une station de gestion pour vous connecter à 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 ou Telnet pour communiquer avec iDRAC, veillez à :

1. Configurer le BIOS pour activer la console série
2. Configurer SOL dans iDRAC
3. Activer SSH ou Telnet en utilisant l'interface Web iDRAC ou RACADM

   Telnet (port 23)/ client SSH (port 22) <--> Connexion WAN <--> iDRAC

   Le SOL basé sur IPMI, qui utilise le protocole SSH ou Telnet, évite d'avoir à utiliser un utilitaire supplémentaire, car la conversion série-réseau s'effectue dans l'iDRAC. La console SSH ou Telnet 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 la console SSH ou Telnet.

Tâches associées

Utilisation de SOL depuis PuTTY sous Windows , page 122
Utilisation de SOL depuis OpenSSH ou Telnet sur Linux , page 123

Utilisation de SOL depuis PuTTY sous Windows

REMARQUE : Si nécessaire, vous pouvez changer le délai d'attente SSH ou Telnet par défaut dans **Présentation générale** > **Paramètres iDRAC** > **Réseau** > **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 | -telnet] <login name>@<iDRAC-ip-address> <port number>
   ```

   REMARQUE : Le numéro de port est facultatif. Il est nécessaire uniquement lorsque le numéro de port est réaffecté.

2. Exécutez la commande `console com2` ou `connect` pour démarrer SOL et le système géré.

   Une session SOL depuis la station de gestion vers le système géré à l'aide du protocole SSH ou Telnet, est ouverte. Pour accéder à la console de ligne de commande iDRAC, suivez la séquence de touche ÉCHAP. Comportement de connexion de Putty et SOL :
   - Lors de l'accès au système géré via putty au cours du POST, si les touches de fonction et l'option de pavé de touches dans putty sont définies sur :
     - VT100+ — F2 passe, mais pas F12

- ESC[n~ — F12 passe, mais pas F2
- Dans Windows, l'ouverture de la console EMS (Emergency Management System) immédiatement après le redémarrage de l'hôte, peut endommager le terminal SAC (Special Admin Console). Quittez la session SOL, fermez le terminal, ouvrez un autre terminal et démarrez la session SOL en utilisant la même commande.

Concepts associés

Déconnexion d'une session SOL dans la console de ligne de commande d'iDRAC , page 124

Utilisation de SOL depuis OpenSSH ou Telnet sur Linux

Pour démarrer SOL depuis OpenSSH ou Telnet sur une station de gestion Linux :

REMARQUE : Si nécessaire, vous pouvez modifier le délai d'attente par défaut des sessions SSH ou Telnet dans **Overview (Présentation)** > **iDRAC Settings (Paramètres iDRAC)** > **Network (Réseau)** > **Services**.

1. Démarrez un shell.
2. Connectez-vous à iDRAC à l'aide de la commande suivante :
   - Pour SSH : ssh *<adresse IP iDRAC>* -l *<nom de connexion>*
   - Pour Telnet : telnet *<adresse IP iDRAC>*

   REMARQUE : Si vous avez remplacé le numéro de port par défaut (port 23) du service Telnet par un autre numéro de port, ajoutez le numéro de port à la fin de la commande Telnet.

3. Entrez l'une des commandes suivantes depuis l'invite de commande pour démarrer SOL :
   - `connect`
   - `console com2`

   Cela permet de connecter iDRAC au port SOL du système géré. Une fois qu'une session SOL est établie, la console de ligne de commande iDRAC n'est pas disponible. Suivez la séquence d'échappement correctement pour ouvrir la console de ligne de commande iDRAC. La séquence d'échappement est également affichée à l'écran dès l'ouverture d'une session SOL. Quand le système géré est éteint, l'établissement d'une session SOL peut prendre du temps.

   REMARQUE : Vous pouvez utiliser console com1 ou console com2 pour démarrer SOL. Redémarrez le serveur pour établir la connexion.

   La commande `console -h com2` affiche le contenu du tampon de l'historique série avant d'attendre une entrée à partir du clavier ou de nouveaux caractères du port série.

   La taille par défaut maximale du tampon d'historique est de 8 192 caractères. Vous pouvez réduire ce nombre avec cette commande :

   ```
   racadm set iDRAC.Serial.HistorySize <number>
   ```

4. Quittez la session SOL pour fermer une session SOL active.

Tâches associées

Utilisation de la console virtuelle Telnet , page 123
Configuration de la touche Retour arrière de la session Telnet , page 124
Déconnexion d'une session SOL dans la console de ligne de commande d'iDRAC , page 124

Utilisation de la console virtuelle Telnet

Certains clients Telnet sur les systèmes d'exploitation Microsoft peuvent ne pas afficher correctement l'écran de configuration du BIOS lorsque la console virtuelle du BIOS est configurée pour l'émulation VT100/VT220. Dans ce cas, faites passer la console du BIOS en mode ANSI pour mettre à jour l'affichage. Pour exécuter cette opération dans le menu de configuration du BIOS, sélectionnez **Console virtuelle** > **Type de terminal distant** > **ANSI**.

Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console virtuelle redirigée sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement ; sinon, certains écrans de texte risquent d'être illisibles.

Pour utiliser la console virtuelle Telnet :

1. Activez **Telnet** dans **Services du composant Windows.**

2. Connectez-vous à iDRAC à l'aide de la commande :

```
telnet <IP address>:<port number>
```

Paramètre	Description
<IP address>	Adresse IP de l'iDRAC
<port number>	Numéro de port telnet (si vous utilisez un nouveau port)

Configuration de la touche Retour arrière de la session Telnet

Selon le client Telnet, l'utilisation de la touche Retour arrière peut générer des résultats inattendus. Par exemple, la session peut renvoyer `^h`. Toutefois, la plupart des clients Telnet Microsoft et Linux peuvent être configurés pour utiliser cette touche.

Pour configurer une session Linux Telnet pour qu'elle utilise la touche <Retour arrière>, ouvrez une invite de commande et tapez `stty erase ^h`. Dans l'invite, tapez `telnet`.

Pour configurer les clients Telnet Microsoft pour qu'ils utilisent la touche Retour arrière :

1. Ouvrez une fenêtre d'invite de commande (si nécessaire).
2. Si vous n'exécutez pas une session Telnet, tapez `telnet`. Si vous utilisez une session Telnet, appuyez sur Ctrl+].
3. Depuis l'invite, tapez `set bsasdel`.
   Le message `Backspace will be sent as delete` s'affiche.

Déconnexion d'une session SOL dans la console de ligne de commande d'iDRAC

Les commandes de déconnexion d'une session SOL reposent sur l'utilitaire. Vous pouvez quitter l'utilitaire uniquement lorsqu'une session SOL est complètement terminée.

Pour déconnecter une session SOL, 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.
- Pour quitter une session SOL à partir de Telnet sur Linux, maintenez enfoncées les touches Ctrl+].
  Une invite Telnet s'affiche. Tapez `quit` pour quitter Telnet.

Si une session SOL n'est pas terminée complètement dans l'utilitaire, d'autres sessions SOL peuvent ne pas être disponibles. Pour résoudre le problème, terminez la console de ligne de commande dans l'interface web sous **Présentation générale** > **Paramètres iDRA** > **Sessions**.

Communication avec l'iDRAC à l'aide d'IPMI sur LAN

Vous devez configurer IPMI sur LAN pour iDRAC afin d'activer ou désactiver les commandes IPMI sur les canaux LAN vers des systèmes externes. S'il n'est pas configuré, les systèmes externes ne peuvent pas communiquer avec le serveur iDRAC à l'aide de commandes IPMI.

REMARQUE : À partir de l'iDRAC v2.30.30.30 ou version ultérieure, IPMI prend en charge également le protocole d'adresse IPv6 pour les systèmes d'exploitation Linux.

Configuration d'IPMI sur LAN en utilisant l'interface Web

Configurez IPMI sur le LAN :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau**.
   La page **Réseau** s'affiche.
2. Sous les **paramètres IPMI**, définissez les valeurs des attributs et cliquez sur **Appliquer**.

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

   Les paramètres IPMI sur le LAN sont définis.

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 en utilisant l'interface IPMI sur le LAN. Pour plus d'informations, voir les spécifications IPMI 2.0 sur le site **intel.com**.

2. Mettez à jour les privilèges du canal IPMI.

```
racadm set iDRAC.IPMILan.PrivLimit <level>
```

Paramètre	Niveau de privilège
<level> = 2	Utilisateur
<level> = 3	Opérateur
<level> = 4	Administrateur

3. Si nécessaire, définissez la clé de chiffrement du canal LAN IPMI.

```
racadm set iDRAC.IPMILan.EncryptionKey <key>
```

Paramètre	Description
<key>	Clé de chiffrement à 20 caractères dans un format hexadécimal valide.

REMARQUE : iDRAC IPMI prend en charge le protocole RMCP+. Pour en savoir plus, voir les spécifications IPMI 2.0 sur le site **intel.com**.

Activation ou désactivation de l'interface distante RACADM

Vous pouvez activer ou désactiver RACADM à distance à l'aide de l'interface web d'iDRAC ou de RACADM. Vous pouvez exécuter jusqu'à cinq sessions de RACADM à distance simultanément.

REMARQUE : L'interface distante RACADM est activée par défaut.

Activation ou désactivation de l'interface distante RACADM à l'aide de l'interface web

1. Dans l'interface web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **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.

Activation ou désactivation de l'interface RACADM distante à l'aide de RACADM

REMARQUE : Il est recommandé d'exécuter ces commandes sur le système local.

- Pour désactiver l'interface RACADM distante :

```
racadm set iDRAC.Racadm.Enable 0
```

- Pour activer l'interface RACADM distante :

```
racadm set iDRAC.Racadm.Enable 1
```

Désactivation de l'interface locale RACADM

Par défaut, l'interface locale RACADM est activée. Pour la désactiver, voir Désactivation de l'accès pour modifier les paramètres de configuration d'iDRAC sur le système hôte.

Activation d'IPMI sur un système géré

Sur un système géré, utilisez Dell Open Manage Server Administrator pour activer ou désactiver IPMI. Pour plus d'informations, voir le *Dell Open Manage Server Administrator's User Guide* (Guide d'utilisation de l'utilitaire Dell OpenManage Server Administrator) à l'adresse **dell.com/support/manuals**.

REMARQUE : À partir de l'iDRAC v2.30.30.30 ou version ultérieure, IPMI prend en charge le protocole d'adresse IPv6 pour les systèmes d'exploitation Linux.

Configuration de Linux pour la console série pendant le démarrage

Les étapes suivantes sont spécifiques de GRUB (Linux GRand Unified Bootloader). Des modification similaires sont nécessaires si un chargeur de démarrage différent est utilisé.

REMARQUE : Lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console virtuelle redirigée, sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement. Sinon, certains écrans de texte risquent d'être illisibles.

Modifiez le fichier **/etc/grub.conf** 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/sdal
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. Pour activer plusieurs options GRUB afin de démarrer des sessions de console virtuelle via la connexion RAC série, ajoutez les lignes suivantes à toutes les options :

```
console=ttyS1,115200n8r console=tty1
```

   Dans l'exemple, `console=ttyS1,57600` a été ajouté à la première option.

   REMARQUE : Si le chargeur de démarrage ou le système d'exploitation fournissent la redirection série (comme GRUB ou Linux), le paramètre **Redirection après démarrage** du BIOS doit être désactivé, cela afin d'éviter d'éventuels états de concurrence de plusieurs composants cherchant à 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 : Uutilisez la séquence de touches d'arrêt (~B) pour exécuter les commandes de touches **Magic SysRq** Linux sur une console série à l'aide de l'outil IPMI.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Schémas cryptographiques SSH pris en charge

Pour communiquer avec iDRAC en utilisant le protocole SSH, iDRAC prend en charge les schémas cryptographiques répertoriés dans le tableau suivant.

Tableau 16. Schémas cryptographiques SSH

Type de schéma	Algorithmes
Cryptographie asymétrique	
Clé publique	ssh-rsa ecdsa-sha2-nistp256
Cryptographie symétrique	
Échange de clés	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1
Chiffrement	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com
MAC	hmac-sha1 hmac-ripemd160 umac-64@openssh.com
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

iDRAC prend en charge l'authentification par clé publique (PKA) sur SSH. Cette fonction est disponible sous licence. Lorsque PKA sur SSH est configuré et utilisé correctement, vous devez entrer le nom d'utilisateur lorsque vous ouvrez une session dans iDRAC. Cela est pratique pour configurer des scripts automatiques qui exécutent diverses fonctions. Les clés téléchargées doivent être de format RFC 4716 ou OpenSSH. Sinon, vous devez les convertir en ce format.

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.

Quel que soit le cas, une paire de clés privée et publique doit être générée sur la station de gestion. La clé publique est téléversée vers l'utilisateur local iDRAC et la clé privée est utilisée par le client SSH pour établir la relation de confiance entre la station de gestion et 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 normalement réservé aux utilisateurs membres du groupe d'utilisateurs Administrateur sur iDRAC. Toutefois, les utilisateurs dans le groupe d'utilisateurs « Personnalisé » peuvent recevoir ce privilège. Un utilisateur avec ce privilège peut modifier n'importe quelle configuration d'utilisateur. Ceci inclut la création ou la suppression d'un utilisateur, la gestion des clés SSH des utilisateurs, etc. Par conséquent, affectez ce privilège avec précaution.

PRÉCAUTION : La possibilité de téléverser, afficher et supprimer des clés SSH repose sur le privilège utilisateur de configuration d'utilisateurs. Ce privilège permet aux utilisateurs de configurer la clé SSH d'un autre utilisateur. Par conséquent, affectez ce privilège avec précaution.

Génération de clés publiques pour Windows

Pour utiliser l'application *PuTTY Key Generator* pour créer la clé de base :

1. Démarrez l'application et sélectionnez RSA comme type de clé.
2. Entrez le nombre de bits de la clé. Ce nombre doit être compris entre 2048 et 4096 bits.
3. Cliquez sur **Générer** et déplacez la souris dans la fenêtre en suivant les instructions.
   Les clés sont générées.
4. Vous ne pouvez pas modifier le champ de commentaire de la clé.
5. Entrez une phrase secrète pour protéger la clé.
6. Enregistrez la clé publique et la clé privée.

Génération de clés publiques pour Linux

Pour utiliser l'application *ssh-keygen* afin de créer la clé de base, ouvrez une fenêtre de terminal et, à l'invite du shell, entrez `ssh-keygen -t rsa -b 2048 -C testing`

où :

- `-t` est *rsa*.
- `-b` spécifie la taille du chiffrement binaire comprise entre 2048 et 4096.
- `-C` permet de modifier le commentaire de la clé publique ; l'option est facultative.

REMARQUE : Les options sont sensibles à la casse.

Suivez les instructions. Après l'exécution de la commande, téléversez le fichier public.

PRÉCAUTION : Les clés générées depuis la station de gestion Linux en utilisant ssh-keygen n'ont pas le format 4716. Convertissez les clés dans le format 4716 en utilisant `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Ne changez pas les autorisations du fichiers de clé. La conversion doit être effectuée en utilisant les autorisations par défaut.

REMARQUE : iDRAC ne prend pas en charge le transfert des clés via ssh-agent.

Téléversement de clés SSH

Vous pouvez téléverser jusqu'à quatre clés publiques *par utilisateur* pour les utiliser sur une interface SSH. Avant d'ajouter les clés publiques, veillez à les visualiser si elles sont configurées afin de ne pas les remplacer accidentellement.

Lorsque vous ajoutez de nouvelles clés publiques, vérifiez que les clés existantes ne se trouvent pas dans l'index auquel la nouvelle clé est ajoutée. iDRAC ne vérifie pas que les clés précédentes sont supprimées avant d'ajouter les nouvelles clés. Lorsque vous ajoutez une nouvelle clé, vous pouvez l'utiliser si l'interface SSH est activée.

Téléversement des clés SSH à l'aide de l'interface Web

Pour téléverser des clés SSH :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Authentification des utilisateurs** > **Utilisateurs locaux**.
   La page **Utilisateurs** s'affiche.

2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **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 plus d'informations, voir l'Aide en ligne d'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 locale RACADM : `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- Pour l'interface distance RACADM en utilisant Telnet 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 d'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 telnet/ssh/série.

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, accédez à **Overview** > **iDRAC Settings** > **Network** > **User Authentication** > **Local Users**(Présentation, Paramètres iDRAC, Réseau, Authentification des utilisateurs, Utilisateurs locaux).
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **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.

Affichage des clés SSH à l'aide de l'interface RACADM

Pour afficher les clés SSH, exécutez les commandes suivantes :

- Pour une clé spécifique : `racadm sshpkauth -i <2 to 16> -v -k <1 to 4>`
- Pour toutes les clés : `racadm sshpkauth -i <2 to 16> -v -k all`

Suppression des clés SSH

Avant de supprimer des clés publiques, affichez les clés si elles sont définies afin de ne pas les supprimer par inadvertance.

Suppression de clés SSH à l'aide de l'interface Web

Pour supprimer des clés SSH :

1. Dans l'interface Web, accédez à **Overview** > **iDRAC Settings** > **Network** > **User Authentication** > **Local Users**(Présentation, Paramètres iDRAC, Réseau, Authentification des utilisateurs, Utilisateurs locaux).
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configurations de clés SSH**, sélectionnez **Afficher/Supprimer une ou des clés SSH** et cliquez sur **Suivant**.
   La page **View/Remove SSH Key(s) (Afficher/Supprimer une ou des clés SSH)** affiche les détails des clés.
4. Sélectionnez **Remove for the key(s) you want to delete**, (Supprimer la ou clés désirées), puis cliquez sur **Appliquer**.
   Les clés sélectionnées sont supprimées.

Suppression des clés SSH en utilisant l'interface RACADM

Pour supprimer les clés SSH, exécutez les commandes suivantes :

- Pour une clé spécifique : `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- Pour toutes les clés : `racadm sshpkauth -i <2 to 16> -d -k all`

7

Configuration des comptes et des privilèges des utilisateurs

Vous pouvez configurer des comptes d'utilisateur avec des privilèges spécifiques (*droit basé sur un rôle*) pour gérer le système à l'aide d'iDRAC et maintenir la sécurité du système. Par défaut, iDRAC est configuré avec un compte d'administrateur local. Ce nom par défaut est *racine* et le mot de passe est *calvin*. En tant qu'administrateur, vous pouvez configurer des comptes d'utilisateur pour autoriser d'autres utilisateurs à accéder à iDRAC.

Vous pouvez définir des utilisateurs locaux ou utiliser des services d'annuaire, tels que Microsoft Active Directory ou LDAP, pour définir des comptes d'utilisateur. L'utilisation d'un service d'annuaire permet de disposer d'un emplacement central de gestion des comptes d'utilisateur autorisés.

iDRAC prend en charge l'accès à base de rôle pour les utilisateurs avec un groupe de privilèges associés. Les rôles sont Administrateur, Opérateur, Lecture seule et Aucun. Le rôle définit les privilèges maximaux disponibles.

Concepts associés

Configuration des utilisateurs locaux , page 134
Configuration des utilisateurs d'Active Directory , page 136
Configuration d'utilisateurs LDAP générique , page 153

Sujets :

- Caractères recommandés pour les noms d'utilisateur et mots de passe
- Configuration des utilisateurs locaux
- Configuration des utilisateurs d'Active Directory
- Configuration d'utilisateurs LDAP générique

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.

Utilisez les caractères suivants lors de la création des noms d'utilisateur et mots de passe :

Tableau 17. Caractères recommandés pour les noms d'utilisateur

Caractères	Longueur
0-9 A-Z a-z - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1-16

Tableau 18. Caractères recommandés pour les mots de passe

Caractères	Longueur
0-9 A-Z a-z ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1-20

REMARQUE : Vous pouvez potentiellement créer des noms d'utilisateur et des mots de passe comprenant d'autres caractères. Toutefois, afin de garantir la compatibilité avec toutes les interfaces, Dell vous 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 réseau partage. Le contrôleur iDRAC prend en charge les caractères autorisés pour les informations d'identification du partage réseau en fonction du type de partage, sauf <, > et , (virgule).

REMARQUE : Pour améliorer la sécurité, il est recommandé d'utiliser des mots de passe complexes comprenant au moins huit caractères avec des lettres minuscules, des lettres majuscules, des chiffres et des caractères spéciaux. Il est également recommandé de changer régulièrement les mots de passe, si possible.

Configuration des utilisateurs locaux

Vous pouvez configurer jusqu'à 16 utilisateurs locaux dans iDRAC avec des autorisations d'accès 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. Les noms d'utilisateurs et les mots de passe peuvent être modifiés à l'aide de n'importe quelle interface sécurisée iDRAC (à savoir, l'interface web, RACADM ou WSMAN). Vous pouvez également activer ou désactiver l'authentification SNMPv3 pour chaque utilisateur.

Configuration des utilisateurs locaux à l'aide de l'interface Web d'iDRAC

Pour ajouter et configurer les utilisateurs iDRAC locaux :

REMARQUE : Vous devez disposer de l'autorisation Configurer des utilisateurs pour pouvoir configurer un utilisateur iDRAC.

1. Dans l'interface Web d'iDRAC accédez à **Présentation** > **Paramètres iDRAC** > **Authentification des utilisateurs** > **Utilisateurs locaux.**
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.

   REMARQUE : L'utilisateur 1 est réservé à l'utilisateur anonyme IPMI ; vous ne pouvez pas changer cette configuration.

   La page **Menu principal utilisateur** s'affiche.
3. Sélectionnez **Configurer**, puis cliquez sur **Suivant**.
   La page **Configuration de l'utilisateur** s'affiche.
4. Activez l'ID utilisateur et spécifiez le nom d'utilisateur, le mot de passe et les droits d'accès de l'utilisateur. Vous pouvez également activer l'authentification SNMPv3 pour cet utilisateur. Pour en savoir plus sur les options, voir l'*Aide en ligne d'iDRAC*.
5. Cliquez sur **Appliquer**. L'utilisateur est créé avec les privilèges demandés.

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 batch 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 nouvel iDRAC ou que vous avez utilisé la commande `racadm racresetcfg`, le seul utilisateur en cours est **root** avec le mot de passe **calvin**. La commande `racadm racresetcfg` restaure les valeurs par défaut d'iDRAC.

REMARQUE : Les utilisateurs peuvent être activés et désactivés ensuite. Par conséquent, un utilisateur peut avoir un numéro d'index différent dans chaque iDRAC.

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 =, ce numéro d'index est pris.

REMARQUE : Vous pouvez également taper `racadm get -f <monfichier.cfg>` et affichez ou modifiez le fichier **monfichier.cfg** qui contient tous les paramètres de configuration d'iDRAC.

Pour activer l'authentification SNMP v3 d'un utilisateur, utilisez les objets **SNMPv3AuthenticationType**, **SNMPv3Enable**, **SNMPv3PrivacyType**. Pour en savoir plus, voir le *RACADM Command Line Interface Guide* (Guide de l'interface de ligne de commande RACADM) disponible à l'adresse **dell.com/idracmanuals**.

Si vous utilisez le fichier XML de configuration, 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 référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 que l'utilisateur n'a aucun privilège activé. Pour obtenir une liste des valeurs de masque binaire valides-pour des privilèges utilisateur spécifiques, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 fonction sous licence.

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

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.

Les noms de rôles et de privilèges utilisés dans iDRAC ont changé au fil des générations de serveurs. Les noms de rôle sont :

Tableau 19. Rôles iDRAC

Génération en cours	Génération antérieure	Privilèges
Administrateur	Administrateur	Connexion, Configurer, Configurer des utilisateurs, Journaux, Contrôler le système, Accéder à la console virtuelle, Accéder à Média Virtuel, Opérations système, Déboguer
Opérateur	Utilisateur privilégié	Connexion, Configurer, Configurer des utilisateurs, Journaux, Contrôler le système, Accéder à la console virtuelle, Accéder à Média Virtuel, Opérations système, Déboguer
Lecture seule	Utilisateur invité	Connexion
Aucun	Aucun	Aucun

Tableau 20. Privilèges utilisateur iDRAC

Génération en cours	Génération antérieure	Description
Connexion	Connexion à iDRAC	Permet à l'utilisateur de se connecter à iDRAC.
Configuration	Configurer iDRAC	Permet à l'utilisateur de configurer iDRAC.
Configurer des utilisateurs	Configurer des utilisateurs	Donne la possibilité à l'utilisateur d'autoriser des utilisateurs à d'accéder au système.
Journaux	Effacer des journaux	Permet à l'utilisateur d'effacer uniquement le journal des événements système (SEL).
Contrôle du système	Exécuter les commandes de contrôle du serveur	Permet d'effectuer un cycle d'alimentation sur le système hôte.
Accéder à la console virtuelle	Accéder à la redirection de la console (pour les serveurs lames) Accéder à la console virtuelle (pour les serveurs en rack et tour)	Permet à l'utilisateur d'exécuter la console virtuelle.
Accéder à Média Virtuel	Accéder à Média Virtuel	Permet à l'utilisateur d'exécuter et d'utiliser Média Virtuel.

Tableau 20. Privilèges utilisateur iDRAC (suite)

Génération en cours	Génération antérieure	Description
Opérations système	Alertes de test	Autorise les événements initialisés et générés par l'utilisateur, et les informations sont envoyées en tant que notification asynchrone et journalisés.
Débogage	Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Concepts associés

Exigences d'utilisation de l'authentification Active Directory pour l'iDRAC , page 137
Mécanismes d'authentification Active Directory pris en charge , page 139

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. Voir le site Web Microsoft pour plus d'informations.
- Intégré PKI à l'infrastructure Active Directory. iDRAC utilise le mécanisme d'infrastructure de clé publique (PKI) standard pour s'authentifier en toute sécurité dans Active Directory. Voir le site Web Microsoft pour plus d'informations.
- Activé SSL (Secure Socket Layer) dans tous les contrôleurs de domaine auxquels iDRAC se connecte pour l'authentification dans tous les contrôleurs de domaine.

Tâches associées

Activation de SSL sur un contrôleur de domaine , page 137

Activation de SSL sur un contrôleur de domaine

Lorsqu'iDRAC authentifie les utilisateurs avec un contrôleur de domaine Active Directory, il démarre une session SSL avec le contrôleur de domaine. À ce stade, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (CA) dont le certificat racine est également téléversé vers iDRAC. Pour qu'iDRAC puisse s'authentifier auprès d'*un* contrôleur de domaine, qu'il s'agisse du contrôleur de domaine racine ou enfant, le contrôleur de domaine doit avoir un certificat SSL signé par l'autorité de certification du domaine.

Si vous utilisez Autorité de certification racine d'entreprise Microsoft pour affecter *automatiquement* tous les contrôleurs de domaine à un certificat SSL, vous devez :

1. installer le certificat SSL dans chaque contrôleur de domaine ;
2. exporter le certificat CA racine du contrôleur de domaine vers iDRAC ;
3. importer le certificat SSL du micrologiciel d'iDRAC.

Tâches associées

Installation du certificat SSL pour chaque contrôleur de domaine , page 137
Exportation d'un certificat CA racine de contrôleur de domaine vers l'iDRAC , page 138
Importation du certificat SSL du micrologiciel d'iDRAC , page 138

Installation du certificat SSL pour chaque contrôleur de domaine

Pour installer le certificat SSL pour chaque contrôleur de domaine :

1. Cliquez sur **Démarrer** > **Outils d'administration** > **Stratégie du domaine de sécurité**.
2. Développez le dossier **Règles de clé publique**, cliquez avec le bouton droit de la souris sur **Paramètres de demande automatique de certificat** et cliquez sur **Demande automatique de certificat**.
   L'**Assistant Demande automatique de certificat** s'affiche.
3. Cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.

4. Cliquez sur **Suivant** et sur **Terminer**. Le certificat SSL est installé.

Exportation d'un certificat CA racine de contrôleur de domaine vers l'iDRAC

REMARQUE : Si votre système fonctionne sous Windows 2000 ou que vous utilisez une autorité de certification autonome, les étapes suivantes peuvent être différentes.

Pour exporter le certificat CA racine du contrôleur de domaine vers iDRAC :

1. Localisez le contrôleur de domaine qui exécute le service CA d'entreprise Microsoft.
2. Cliquez sur **Démarrer** > **Exécuter**.
3. Tapez `mmc` et cliquez sur **OK**.
4. Dans la fenêtre **Console 1** (MMC), cliquez sur **Fichier (**ou sur **Console** pour les systèmes Windows 2000**)** et sélectionnez **Ajouter/ Supprimer un snap-in**.
5. Dans la fenêtre **Ajouter/Supprimer un snap-in**, cliquez sur **Ajouter**.
6. Dans la fenêtre **Snap-in autonome**, sélectionnez **Certificats** et cliquez sur **Ajouter**.
7. Sélectionnez **Ordinateur** et cliquez sur **Suivant**.
8. Sélectionnez **Ordinateur local** et cliquez sur **Terminer**, puis sur **OK**.
9. Dans la fenêtre **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 votre système exécute Windows 2000, les étapes suivantes peuvent varier.

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 contient des objets Active Directory personnalisés. Tous les objets de contrôle d'accès sont gérés dans Active Directory. La solution offre une souplesse maximale pour configurer l'accès des utilisateurs dans différents iDRAC avec des niveaux de privilèges différents.

Concepts associés

Présentation d'Active Directory avec le schéma standard , page 139
Présentation d'Active Directory avec schéma étendu , page 142

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.

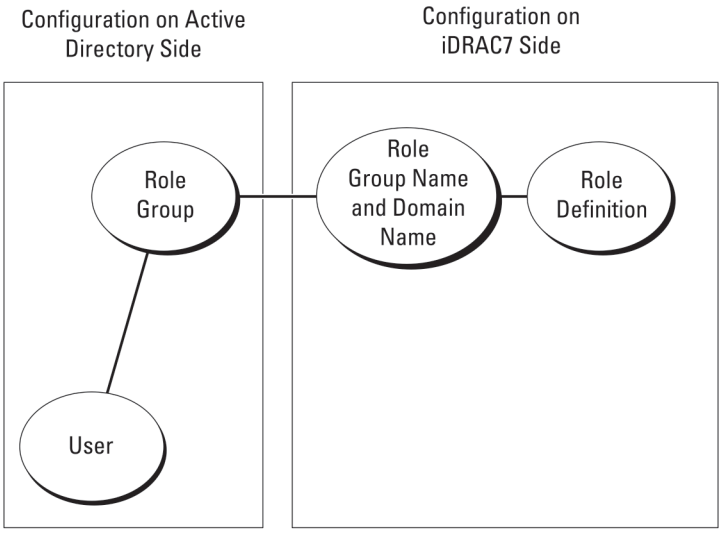


Figure 1. Configuration d'iDRAC avec le schéma standard d'Active Directory

Dans Active Directory, un objet de groupe standard est utilisé comme groupe de rôles. Un utilisateur qui dispose d'un accès iDRAC est membre du groupe de rôles. Pour que cet utilisateur puisse accéder à un iDRAC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés dans l'iDRAC concerné. Le rôle et le niveau de privilège sont définis dans chaque iDRAC et non dans Active Directory. Vous pouvez configurer jusqu'à cinq groupes de rôles dans chaque iDRAC. Le tableau répertorie les privilèges par défaut des groupes de rôles.

Tableau 21. 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,	0x000001ff

Tableau 21. Privilèges par défaut des groupes de rôles (suite)

Groupes de rôles	Niveau de privilège par défaut	Droits accordées	Masque binaire
		Exécuter des commandes de diagnostic	
Groupe de rôles 2	Aucun	Ouvrir une session iDRAC, Configurer iDRAC, Exécuter des commandes de contrôle de serveur, Accéder à la console virtuelle, Accéder à Média Virtuel, Tester les alertes, Exécuter des commandes de diagnostic	0x000000f9
Groupe de rôles 3	Aucun	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 iDRAC. Dans ce scénario impliquant un seul domaine, n'importe quel type de groupe est pris en charge.

Si tous les utilisateurs et groupes de rôles, ou un groupe imbriqué, proviennent de plusieurs domaines, des adresses de serveur de catalogue global doivent être définies dans iDRAC. Dans ce scénario impliquant plusieurs domaines, tous les groupes de rôles et les groupes imbriqués, s'il en existe, doivent être de type Groupe universel.

Configuration d'Active Directory avec le schéma standard

Pour configurer 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 un groupe ou sélectionnez un groupe existant. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour accéder à 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.

Tâches associées

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC , page 140
Configuration d'Active Directory avec le schéma standard à l'aide de RACADM , page 141

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 d'iDRAC accédez à **Présentation** > **Paramètres iDRAC** > **Authentification des utilisateurs** > **Utilisateurs locaux.**
   La page **Services d'annuaire** s'affiche.

2. Sélectionnez l'option **Microsoft Active Directory**, puis cliquez sur **Appliquer**.
   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. Vous pouvez également activer la validation de certificat et téléverser le certificat numérique signé par une autorité de certification, utilisé pendant l'initialisation des connexions SSL lors de la communication avec le serveur Active Directory (AD). Pour ce faire, vous devez définir les contrôleurs de domaine et le nom de domaine complet qualifié du catalogue. Vous le faites dans les étapes suivantes. Le DNS doit être alors configuré correctement dans les paramètres réseau.
5. Cliquez sur **Suivant**.

   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. Définissez également le délai d'attente des réponses d'Active Directory qu'iDRAC doit respecter lors de l'ouverture de session dans iDRAC.

   REMARQUE : Si la validation de certificat est activée, indiquez les adresses de serveur de contrôleur de domaine et le nom de domaine complet du catalogue global. Vérifiez que le DNS est configuré correctement dans**Présentation** > **Paramètres iDRAC** > **Réseau**.

7. Cliquez sur **Suivant**. 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.

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 permissions de groupes de rôles spécifiques, voir Privilèges par défaut des groupes de rôles , page 139.
- Vous devez fournir au moins l'une des trois adresses de contrôleur de domaine. iDRAC tente de se connecter à chacune des adresses configurées l'une après l'autre jusqu'à ce qu'une connexion soit établie. 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 la négociation 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 la négociation 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.

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 meilleures pratiques pour le schéma étendu

Le schéma étendu utilise les objets Association de Dell pour joindre iDRAC et des permissions. Cela vous permet d'utiliser iDRAC en fonction des permissions globales accordées. La liste ACL par défaut des contrôles d'accès des objets Association de Dell permet aux administrateurs Self et Domain de gérer les permissions et la portée des objets iDRAC.

Par défaut, les objets Association de Dell n'héritent pas de toutes les permissions des objets Active Directory parents. Si vous activez l'héritage pour l'objet Association de Dell, les permissions héritées de cet objet Association sont accordées aux utilisateurs et aux groupes sélectionnés. Cela peut entraîner l'octroi à iDRAC de privilèges non prévus.

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 sont une base de données distribuée d'*attributs* et de *classes*. Le schéma Active Directory contient les règles qui déterminent le type de données pouvant être ajouté ou inclus dans la base de données. La classe Utilisateur est un exemple de *classe* stockée dans la base de données. Certains exemples d'attributs de classe peuvent inclure le nom, le prénom, le numéro de téléphone etc. de l'utilisateur. Vous pouvez étendre la base de données Active Directory en ajoutant vos propres *attributs* et *classes* uniques en fonction de vos besoins. Dell a étendu le schéma pour inclure les modifications nécessaires pour prendre en charge l'authentification et l'autorisation de la gestion à distance à l'aide d'Active Directory.

Chaque *attribut* ou *classe* ajouté à un schéma Active Directory existant doit être défini avec un ID unique. Pour gérer les ID uniques dans le secteur, Microsoft gère une base de données d'identificateurs d'objet Active Directory pour que, lorsque les entreprises ajoutent des extensions au schéma, ces extensions soient réputées uniques et n'entrent pas en conflit. Pour étendre le schéma dans Active Directory Microsoft, Dell a reçu des identificateurs d'objet uniques, des extensions de nom uniques et des ID d'attribut liés de manière unique pour les attributs et les classes ajoutés au service d'annuaire :

- L'extension est : `dell`
- L'identificateur d'objet base est `1.2.840.113556.1.8000.1280`
- La plage des ID de liens RAC est `12070 to 12079`

Présentation des extensions de schéma d'iDRAC

Dell a étendu le schéma pour inclure les propriétés *Association*, *Périphérique* et *Privilège*. La propriété *Association* permet de lier des utilisateurs ou des groupes avec un groupe de privilèges à un ou plusieurs périphériques iDRAC. Ce modèle fournit à l'administrateur une souplesse optimale sur les diverses combinaisons d'utilisateurs, de privilèges iDRAC et de périphériques iDRAC sur le réseau sans trop de difficulté.

Pour chaque périphérique iDRAC physique du réseau que vous voulez intégrer à Active Directory pour l'authentification et l'autorisation, créez au moins un objet Association et un objet Périphérique iDRAC. Vous pouvez créer plusieurs objets Association qui peuvent être liés chacun à un nombre illimité d'utilisateurs, de groupes d'utilisateurs ou objets Périphérique iDRAC. Les utilisateurs et les groupes d'utilisateurs iDRAC peuvent être membres de n'importe quel domaine de l'entreprise.

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

L'objet Périphérique iDRAC est le lien au micrologiciel iDRAC pour interroger Active Directory pour l'authentification et l'autorisation. Lorsqu'iDRAC est ajouté au réseau, l'administrateur doit configurer iDRAC et son objet Périphérique avec son nom Active Directory pour que les utilisateurs puissent exécuter l'authentification et l'autorisation avec Active Directory. En outre, l'administrateur doit ajouter 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.

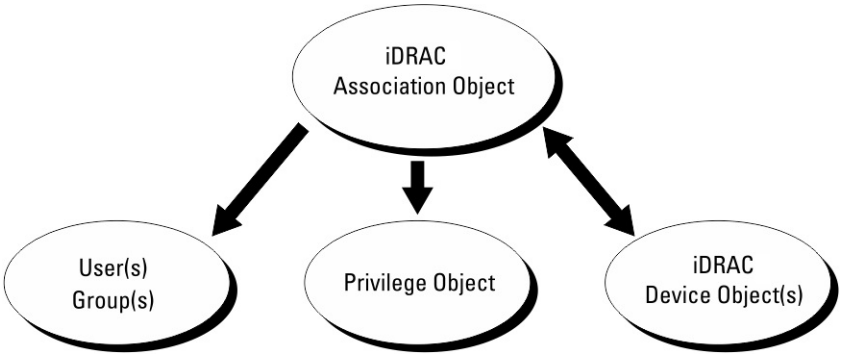


Figure 2. Configuration type pour les objets active directory

Vous pouvez créez un nombre illimité ou réduit d'objets Association. Cependant, vous devez créer au moins un objet Association et vous devez disposer d'un objet Périphérique iDRAC pour chaque périphérique iDRAC du réseau à intégrer à Active Directory pour l'authentification et l'autorisation avec iDRAC.

L'objet Association permet de créer un nombre illimité ou réduit d'utilisateurs, de groupes et d'objets Périphériques iDRAC. Toutefois, l'objet Association contient un seul objet Privilège pour chaque objet Association. L'objet Association connecte les utilisateurs ayant des privilèges sur les périphériques iDRAC.

L'extension Dell au snap-in ADUC MMC permet d'associer l'objet Privilège et les objets iDRAC d'un même domaine à l'objet Association. L'extension Dell ne permet pas d'ajouter un groupe ou un objet iDRAC d'autres domaines comme membre de l'objet Association.

Lors de l'ajout de groupes universels de domaines distincts, créez un objet Association avec une étendue universelle. Les objets Association par défaut créés par l'utilitaire Dell Schema Extender sont des groupes locaux de domaines et ils ne fonctionnent pas avec les groupes universels des autres domaines.

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

Accumulation de privilèges à l'aide du schéma étendu

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

L'illustration suivante montre un exemple d'accumulation de privilèges à l'aide du schéma étendu.

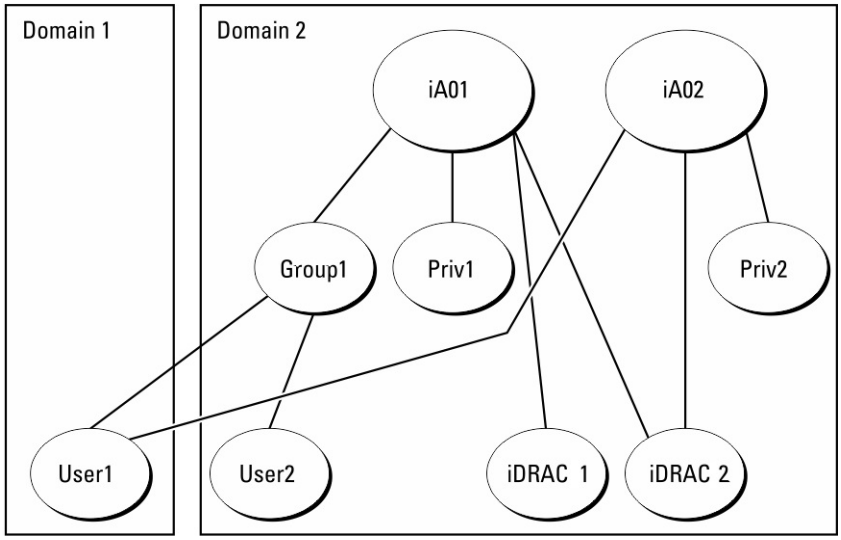


Figure 3. Accumulation de privilèges pour un utilisateur

L'illustration montre deux objets Association, A01 et A02. L'utilisateur 1 est associé à iDRAC2 via les deux objets associés.

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

Dans cet exemple, l'utilisateur 1 dispose des privilèges Priv1 et Priv2 sur iDRAC2. L'utilisateur 1 dispose des privilèges Priv1 sur iDRAC1 uniquement. L'utilisateur 2 dispose des privilèges Priv1 sur iDRAC1 et iDRAC2. En outre, cette figure montre que l'utilisateur 1 peut se trouver dans un domaine différent et qu'il 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.

Concepts associés

Présentation d'Active Directory avec schéma étendu , page 142
Installation de l'extension Dell dans le snap-in Utilisateurs et ordinateurs Active Directory , page 148
Ajout d'utilisateurs iDRAC et de leurs privilèges à Active Directory , page 149

Tâches associées

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web iDRAC , page 151
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM , page 151

Extension du schéma Active Directory

L'extension du schéma Active Directory ajoute à ce schéma une unité organisationnelle Dell, des classes et des attributs de schéma, des exemples de privilèges et des objets Association. Avant d'étendre le schéma, vérifiez que vous disposez bien des privilèges d'administration de schéma dans le rôle de propriétaire FSMO (Flexible Single Master Operation) du contrôleur de domaine principal dans la forêt de domaines.

REMARQUE : Veillez à utiliser l'extension de schéma de ce produit s'il est différent de la génération précédente de produits RAC. Le schéma antérieur ne fonctionne pas avec ce produit.

REMARQUE : L'extension du nouveau schéma n'a pas d'impact sur les versions antérieures du produit.

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

- utilitaire Dell Schema Extender ;
- fichier script LDIF.

Si vous utilisez le fichier script LDIF, l'unité 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 :

- LecteurDVD:`\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files`
- <LecteurDVD>: `\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender`

Pour utiliser les fichiers LDIF, consultez les instructions du fichier « Lisez-moi » qui se trouve dans le répertoire **LDIF_Files**.

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

Utilisation de Dell Schema Extender

PRÉCAUTION : Dell Schema Extender utilise le fichier SchemaExtenderOem.ini. Pour assurer le bon fonctionnement de Dell Schema Extender, ne modifiez pas le nom de ce fichier.

1. Dans l'écran **d'accueil**, cliquez sur **Suivant**.
2. Lisez l'avertissement 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 déterminer si les classes et les attributs Classes et attributs existent. Voir la documentation Microsoft pour plus d'informations sur MMC et le snap-in de schéma Active Directory.

Classes et attributs

Tableau 22. 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

Tableau 22. Définitions de classe pour les classes ajoutées au schéma Active Directory (suite)

Nom de classe	Numéro d'identification d'objet (OID) attribué
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 23. DelliDRACdevice class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Représente le dispositif Dell iDRAC. IDRAC doit être configuré sous la forme delliDRACDevice dans Active Directory. Cette configuration permet à iDRAC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 24. delliDRACAssociationObject Class

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

Tableau 25. 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 26. 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 27. 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 28. Liste des attributs ajoutés au schéma Active Directory

Nom/Description de l'attribut	OID attribué/Identifiant d'objet de syntaxe	Valeur unique
dellPrivilegeMember Liste des objets dellPrivilege qui appartiennent à cet attribut.	1.2.840.113556.1.8000.1280.1.1.2.1 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Liste des objets dellRacDevice et DelliDRACDevice appartenant 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 a les droits Ouvrir une session sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.3 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si l'utilisateur a les droits Configuration de carte sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.4 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si l'utilisateur a les droits Configuration d'utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE

Tableau 28. Liste des attributs ajoutés au schéma Active Directory (suite)

Nom/Description de l'attribut	OID attribué/Identifiant d'objet de syntaxe	Valeur unique
TRUE si l'utilisateur a les droits Effacement de journal sur le périphérique.	Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser TRUE si l'utilisateur a les droits Réinitialisation de serveur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.7 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si l'utilisateur a les droits Console virtuelle sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.8 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si l'utilisateur a les droits Média Virtuel sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.9 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si l'utilisateur a les droits Utilisateur pour l'alerte test sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si l'utilisateur a les droits Administrateur pour la commande de débogage sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.11 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La version de schéma actuelle est utilisée pour mettre à jour le schéma.	1.2.840.113556.1.8000.1280.1.1.2.12 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Cet attribut est le type de RAC actuel pour l'objet delliDRACDevice et le lien précédent vers le lien suivant dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste des objets dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière avec 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 de systèmes en utilisant le DVD *Dell Systems Management Tools and Documentation* , vous pouvez étendre le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** pendant l'installation. Consultez le guide d'installation rapide de Dell OpenManage pour plus d'instructions sur l'installation du logiciel de gestion de systèmes. Pour les systèmes d'exploitation Windows 64 bits, le propramme d'installation du snap-in se trouve sous :

<lecteur DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez la documentation Microsoft.

Ajout d'utilisateurs 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 Périphérique, 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.

Concepts associés

Ajout d'objets à un objet Association , page 150

Tâches associées

Création d'un objet Périphérique iDRAC , page 149
Création d'un objet Privilège , page 149
Création d'un objet Association , page 149

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 entrez lors de la configuration des propriétés Active Directory à l'aide de l'interface Web d'iDRAC Web.
4. Sélectionnez **Objet Périphérique** iDRAC, puis cliquez sur OK.

Création d'un objet Privilège

Pour créer un objet Privilège :

REMARQUE : Vous devez créer un objet Privilège dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** > **Dell Remote Management Object Advanced**.
   La fenêtre **Nouvel objet** s'affiche.
3. Entrez le nom du nouvel objet.
4. Sélectionnez **Objet Privilège**, puis cliquez sur OK.
5. Cliquez avec le bouton droit de la souris sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Privilèges de gestion à distance** pour l'utilisateur ou le groupe.

Création d'un objet Association

Pour créer un objet Association :

REMARQUE : L'objet Association 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.

Tâches associées

Octroi de privilèges d'accès utilisateur pour les objets Association , page 150

Octroi de privilèges d'accès utilisateur pour les objets Association

Octroyez des privilèges d'accès aux utilisateurs authentifiés afin de leur permettre d'accéder aux objets Association créés.

1. Accédez à **Outils d'administration** > **Modifier ADSI**. La fenêtre **Modifier ADSI** s'affiche.
2. Dans le volet de droite, accédez à l'objet Association créé, cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
3. Dans l'onglet **Sécurité**, cliquez sur **Ajouter**.
4. Tapez `Authenticated Users`, cliquez sur **Vérifiez les noms** et sur **OK**. Les utilisateurs authentifiés sont ajoutés à la liste des **groupes et des noms d'utilisateurs**.
5. Cliquez sur **OK**.

Ajout d'objets à un objet Association

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

Vous pouvez ajouter des groupes d'utilisateurs et des périphériques iDRAC.

Tâches associées

Ajout d'utilisateurs ou de groupes d'utilisateurs , page 150
Ajout de privilèges , page 150
Ajout de périphériques iDRAC ou de groupes de périphériques iDRAC , page 150

Ajout d'utilisateurs ou de groupes d'utilisateurs

Pour ajouter des utilisateurs ou des groupes d'utilisateurs :

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

Ajout de privilèges

Pour ajouter des privilèges :

Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs lors de l'authentification sur un périphérique iDRAC. Un seul objet Privilège peut être ajouté à un objet Association.

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Entrez le nom de l'objet Privilège et cliquez sur **OK**.
3. Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs lors de l'authentification sur un périphérique iDRAC. Un seul objet Privilège peut être ajouté à un objet Association.

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 périphérique iDRAC connecté au réseau, qui est disponible pour les utilisateurs et les groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques iDRAC à un objet Association.

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 d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Authentification des utilisateurs** > **Services de répertoire** > **Microsoft Active Directory**.
   La page de résumé **Active Directory** apparaît.
2. Cliquez sur **Configurer Active Directory**.
   La page **Configuration et gestion d'Active Directory - Étape 1 sur 4** s'affiche.
3. Si vous le désirez, vous pouvez activer la validation de certificat et téléverser le certificat numérique signé d'autorité de certification utilisé au cours de l'initialisation des connexions SSL lors de la communication avec le serveur Active Directory (AD).
4. Cliquez sur **Suivant**.
   La page **Configuration et gestion d'Active Directory - Étape 2 sur 4** s'affiche.
5. Définissez les informations d'emplacement des serveurs et des comptes d'utilisateur Active Directory (AD), ainsi que le délai d'attente qui doit s'écouler avant qu'iDRAC reçoive des réponses d'AD au cours du processus d'ouverture de session.

   REMARQUE :
   - Si la validation de certificat est activée, définissez les adresses de serveur de contrôleur de domaine et le nom de domaine complet qualifié (FQDN). Vérifiez que le DNS est correctement défini sous **Présentation** > **Paramètres iDRAC** > **Réseau**.
   - Si l'utilisateur et l'objet iDRAC se trouvent dans un domaine différent, ne sélectionnez pas l'option **Domaine utilisateur de l'ouverture de session**. À la place, sélectionnez **Définir un domaine** et saisissez le nom du domaine sur lequel réside l'objet iDRAC.

6. Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory -Étape 3 sur 4** s'affiche.
7. Sélectionnez **Schéma étendu** et cliquez sur **Suivant**.
   La page **Configuration et gestion d'Active Directory - Étape 4 sur 4** s'affiche.
8. Entrez le nom et l'emplacement de l'objet Périphérique iDRAC dans Active Directory (AD) et cliquez sur **Terminer**.
   Les paramètres Active Directory du mode Schéma étendu sont configurés.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Pour configurer Active Directory avec le schéma étendu en utilisant l'interface RACADM :

1. 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, entrez `servername.dell.com` au lieu de `dell.com`.
   - Vous devez fournir au moins l'une des trois adresses. iDRAC tente de se connecter à chacune des adresses configurées l'une après l'autre jusqu'à ce qu'une connexion soit établie. 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 la négociation 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 la négociation 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 **Présentation** > **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.

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 d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Authentification des utilisateurs** > **Services de répertoire** > **Microsoft Active Directory**.
   La page de résumé **Active Directory** apparaît.
2. Cliquez sur **Tester les paramètres**.
3. Entrez le nom d'un utilisateur de test (par exemple, **nom_utilisateur@domaine.com**) et un mot de passe, puis cliquez sur **Démarrer le test**. Les résultats détaillés du test et le journal du test s'affichent.

   En cas d'échec d'une étape, examinez les détails dans le journal du test pour identifier le problème et une éventuelle solution.

   REMARQUE : Lorsque vous testez les paramètres Active Directory avec la validation de certificat activée, iDRAC impose que le serveur Active Directory soit identifié par le nom de domaine complet qualifié (FQDN) et non pas par une adresse IP. S'il est identifié par une adresse IP, la validation de certificat échoue, car iDRAC ne peut pas communiquer avec le serveur Active Directory.

Test des paramètres Active Directory à l'aide de RACADM

Pour tester les paramètres Active Directory, utilisez la commande `testfeature`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration d'utilisateurs LDAP générique

iDRAC fournit une solution générique permettant de prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol, Protocole léger d'accès aux répertoires). Cette fonction ne nécessite aucune extension de schéma dans les services de répertoire.

Pour rendre la mise en œuvre LDAP iDRAC générique, les points communs entre différents services de répertoire sont utilisés pour regrouper les utilisateurs et adresser ensuite la relation utilisateur-groupe. L'action de service de répertoire est le schéma. Par exemple, ils peuvent avoir des noms d'attribut différents pour le groupe, l'utilisateur et le lien entre l'utilisateur et le groupe. Ces actions peuvent être configurées dans iDRAC.

REMARQUE : Les connexions Authentification bifactorielle (TFA) et directe SSO (Single Sign-On) ne sont pas prises en charge pour le service d'annuaire LDAP générique.

Tâches associées

Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web d'iDRAC , page 153
Configuration du service d'annuaire LDAP générique à l'aide de RACADM , page 154

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 iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Authentification utilisateur** > **Services de répertoire** > **Service de répertoire LDAP générique**.
   La page **Configuration et gestion de LDAP générique** affiche les paramètres LDAP générique actuels.
2. Cliquez sur **Configurer LDAP générique**.
3. 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.

   REMARQUE : Dans cette version, les liaisons LDAP basées sur un port non-SSL ne sont pas prises en charge. Seul LDAP over SSL est pris en charge.

4. Cliquez sur **Suivant**.
   La page **Configuration et gestion LDAP génériques - Étape 2/3** s'affiche.
5. Activez l'authentification LDAP générique et définissez les iinformations d'emplacement des serveurs et des comptes d'utilisateur LDAP générique.

   REMARQUE : Si la validation de certificat est activée, définissez le nom de domaine complet qualifié du serveur LDAP et vérifiez qu'il est correctement défini sous **Présentation générale** > **Paramètres iDRAC** > **Réseau**.

   REMARQUE : Dans cette version, les groupes imbriqués ne sont pas pris en charge. Le micrologiciel recherche le membre direct du groupe pour le faire correspondre au nom de domaine d'utilisateur. En outre, un seul domaine est pris en charge. Les domaines croisés ne sont pas pris en charge.

6. Cliquez sur **Suivant**.
   La page **Configuration et gestion LDAP générique - Étape 3a/3** s'affiche.
7. Cliquez sur **Groupe de rôles**.
   La page **Configuration et gestion LDAP générique - Étape 3a/3** s'affiche.
8. Définissez le nom distinct du groupe et les privilèges du groupe et cliquez sur **Appliquer**.

REMARQUE : Si vous utilisez Novell eDirectory et que vous avez utilisé les caractères #(hachage), " (guillemets doubles), ; (point-virgule), > (supérieur à), , (virgule) ou <(inférieur à) pour le nom de domaine de groupe, vous devez utiliser le caractères d'échappement.

Les paramètres de groupe de rôles sont enregistrés. La page **Configuration et gestion LDAP générique - Étape 3a/3** affiche les paramètres du groupe de rôles.

9. Si vous voulez configurer d'autres groupes de rôles, répétez les étapes 7 et 8.
10. Cliquez sur **Terminer**. Le service d'annuaire LDAP générique est configuré.

Configuration du service d'annuaire LDAP générique à l'aide de RACADM

Pour configurer le service d'annuaire LDAP, utilisez les objets des groupes `iDRAC.LDAP` et `iDRAC.LDAPRole`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 d'iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Authentification des utilisateurs** > **Services de répertoire** > **Services de répertoire LDAP générique**.
   La page **Configuration et gestion de LDAP générique** affiche les paramètres LDAP générique actuels.
2. Cliquez sur **Tester les paramètres**.
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.

Test des paramètres du service d'annuaire LDAP à l'aide de RACADM

Pour tester les paramètres du service d'annuaire LDAP, utilisez la commande `testfeature`. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

8

Configuration de l'iDRAC pour la connexion directe 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 la connexion directe (SSO) (pour les utilisateurs Active Directory.) La connexion directe et la connexion avec une carte à puce sont des fonctions disponibles sous licence.

iDRAC pend en charge l'authentification Active Directory basée sur Kerberos pour pendre en charge la connexion directe et la connexion avec une carte à puce. Pour plus d'informations sur Kerberos, voir le site Web de Microsoft.

Tâches associées

Configuration d'ouverture de session par connexion directe (SSO) iDRAC pour les utilisateurs Active Directory , page 157
Configuration d'ouverture de session iDRAC par carte à puce pour les utilisateurs locaux , page 158
Configuration de la connexion par carte à puce iDRAC pour les utilisateurs Active Directory , page 159

Sujets :

- Exigences d'ouverture de session Active Directory par connexion directe ou carte à puce
- Configuration d'ouverture de session par connexion directe (SSO) iDRAC pour les utilisateurs Active Directory
- Configuration d'ouverture de session iDRAC par carte à puce pour les utilisateurs locaux
- Configuration de la connexion par carte à puce iDRAC pour les utilisateurs Active Directory
- Activation ou désactivation de l'ouverture de session par carte à puce

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 iDRAC avec l'heure du contrôleur de domaine Active Directory. Si vous ne le faites pas, l'authentification kerberos sur iDRAC échoue. Vous pouvez utiliser le fuseau horaire et la fonction NTP pour synchroniser l'heure. Pour ce faire, voir Configuring time zone and ntp (Configuration du fuseau horaire et du NTP).
- Enregistrez iDRAC comme un ordinateur dans le domaine racine Active Directory.
- Générez un fichier keytab en utilisant l'outil ktpass.
- Pour activer la connexion directe pour le schéma étendu, vérifiez que l'option **Trust this user for delegation to any service (Kerberos only) (Faire confiance à cet utilisateur pour la délégation à n'importe quel service [Kerberos uniquement])** est sélectionnée dans l'onglet **Delegation (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, voir Configuration des navigateurs web pris en charge , page 59.

  REMARQUE : Google Chrome et Safari ne prennent pas en charge Active Directory pour la connexion SSO.

Tâches associées

Enregistrement d'iDRAC en tant qu'ordinateur dans un domaine racine Active Directory , page 156
Génération d'un fichier Keytab Kerberos , page 156
Création d'objets Active Directory et fourniture de privilèges , page 156

Enregistrement d'iDRAC en tant qu'ordinateur dans un domaine racine Active Directory

Pour enregistrer iDRAC dans un domaine racine Active Directory :

1. Cliquez sur **Présentation générale** > **Paramètres iDRAC** > **Réseau** > **Réseau**.
   La page **Réseau** s'affiche.
2. Entrez une adresse IP de **serveur DNS préféré/secondaire**. Cette valeur est une adresse IP de serveur DNS qui fait partie du domaine racine.
3. Sélectionnez **Enregistrer iDRAC auprès du DNS.**
4. Spécifiez un **nom de domaine DNS**.
5. Vérifiez que la configuration DNS du réseau correspond aux informations DNS d'Active Directory.

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

Génération d'un fichier Keytab Kerberos

Pour prendre en charge l'authentification d'ouverture de session par connexion directe (SSO) et avec une carte à puce, iDRAC prend en charge la configuration pour s'activer comme service « kerberisé » sur un réseau Windows Kerberos. La configuration Kerberos sur iDRAC implique les mêmes étapes que la configuration d'un service Kerberos non–Windows Server comme principal de sécurité dans Windows Server Active Directory.

L'outil *ktpass* (fourni par Microsoft sur le CD/DVD d'installation du serveur) permet de créer les liaisons SPN (Service Principal Name) à un compte d'utilisateur et d'exporter les données d'approbation vers un fichier *keytab* Kerberos de type MIT qui établit une relation de confiance entre un utilisateur ou un système externe et le centre de distribution de clés (KDC). Le fichier keytab contient une clé cryptographique qui permet de crypter les informations entre le serveur et le centre KDC. L'outil ktpass permet aux services UNIX, qui prennent en charge l'authentification Kerberos, d'utiliser les fonctions d'interopérabilité fournies par un service KDC Kerberos Windows Server. Pour plus d'informations sur l'utilitaire **ktpass**, voir le site Web Microsoft à l'adresse **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

Avant de générer un fichier keytab, vous devez créer un compte d'utilisateur Active Directory à utiliser avec l'option **-mapuser** de la commande `ktpass`. En outre, vous devez avoir le même nom que le nom DNS iDRAC vers lequel vous téléversez le fichier keytab généré.

Pour générer un fichier keytab à l'aide de l'outil ktpass :

1. Exécutez l'utilitaire *ktpass* sur le contrôleur de domaine (serveur Active Directory) sur lequel vous souhaitez adresser iDRAC à un compte utilisateur dans Active Directory.
2. Utilisez la commande ktpass suivante pour créer le fichier keytab Kerberos :

   ```
   C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -mapuser
   DOMAINNAME\username -mapOp set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
   [password] -out c:\krbkeytab
   ```

   Le type de cryptage est AES256-SHA1. Le type de principal est KRB5_NT_PRINCIPAL. La propriété **Utiliser les types de cryptage AES 256 pour ce compte** doit être activée dans les propriétés du compte d'utilisateur auquel le nom de principal de service est adressé.

   REMARQUE : Utilisez des minuscules pour le **Nom iDRAC** et le **Nom principal de service**. Utilisez des majuscules pour le nom de domaine, comme indiqué dans l'exemple.

3. Exécutez la commande suivante :

   ```
   C:\>setspn -a HTTP/iDRACname.domainname.com username
   ```

   Un fichier keytab est généré.

   REMARQUE : En cas de problème avec l'utilisateur iDRAC pour lequel le fichier keytab est créé, créez un nouvel utilisateur et un nouveau fichier keytab. Si vous exécutez de nouveau le fichier créé initialement, il ne se configure pas correctement.

Création d'objets Active Directory et fourniture de privilèges

Procédez comme suit pour la connexion directe avec un schéma étendu Active Directory :

1. Créez l'objet Périphérique, l'objet Privilège et l'objet Association sur le serveur Active Directory.

2. Définissez des privilèges d'accès à l'objet Privilège créé. Il est recommandé de ne pas fournir les privilèges d'administrateur afin qu'aucune vérification de sécurité ne soit ignorée.
3. Associez l'objet Périphérique et l'objet Privilègeà l'aide de l'objet Association.
4. Ajoutez l'utilisateur SSO précédent (utilisateur de connexion) à l'objet Périphérique.
5. Fournissez un privilège d'accès aux *utilisateurs authentifiés* afin de leur permettre d'accéder à l'objet Association créé.

Concepts associés

Ajout d'utilisateurs iDRAC et de leurs privilèges à Active Directory , page 149

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.

Concepts associés

Exigences d'ouverture de session Active Directory par connexion directe ou carte à puce , page 155

Tâches associées

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC , page 140
Configuration d'Active Directory avec le schéma standard à l'aide de RACADM , page 141
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web iDRAC , page 151
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM , page 151

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. Déterminez si le nom DNS iDRAC correspond au nom de domaine complet qualifié iDRAC. Pour ce faire, dans l'interface Web iDRAC, accédez à **Présentation** > **Paramètres iDRAC** > **Réseau** > **Réseau** et vérifiez la propriété du **nom de domaine DNS**.
2. Lors de la configuration d'Active Directory pour définir un compte d'utilisateur basé sur le schéma standard ou étendu, exécutez les deux opérations supplémentaires suivantes pour configurer la connexion directe :
   - Téléversez le fichier keytab sur la page **Gestion et configuration Active Directory - étape 1 sur 4**.
   - Sélectionnez l'option **Activer la connexion directe** dans la page **Gestion et configuration Active Directory - Étape 2 sur 4**.

Configuration d'ouverture de session 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
```

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

Concepts associés

Obtention de certificats , page 98
Téléversement du certificat d'utilisateur de carte à puce , page 158
Activation ou désactivation de l'ouverture de session par carte à puce , page 159

Téléversement du certificat d'utilisateur de carte à puce

Avant de téléverser le certificat d'utilisateur, veillez à exporter au format Base64 le certificat du fournisseur de la carte à puce. Les certificats SHA-2 sont également pris en charge.

Concepts associés

Obtention de certificats , page 98

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 d'iDRAC, accédez à **Présentation** > **Paramètres d'iDRAC** > **Réseau** > **Authentification des utilisateurs** > **Utilisateurs locaux**.
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configurations de cartes à puce**, sélectionnez **Téléverser un certificat d'utilisateur** et cliquez sur **Suivant**.
   La page **Téléversement d'un certificat d'utilisateur** s'affiche.
4. Accédez au certificat d'utilisateur en base 64, sélectionnez-le et cliquez sur **Appliquer**.

Téléversement d’un certificat d’utilisateur de carte à puce en à l’aide de RACADM

Pour téléverser un certificat d’utilisateur de carte à puce, utilisez l’objet **usercertupload**. Pour en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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.

Concepts associés

Obtention de certificats , page 98

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 d'iDRAC, accédez à **Présentation** > **Paramètres d'iDRAC** > **Réseau** > **Authentification des utilisateurs** > **Utilisateurs locaux**.
   La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.
   La page **Menu principal utilisateur** s'affiche.
3. Sous **Configurations de 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 référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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*.

Concepts associés

Activation ou désactivation de l'ouverture de session par carte à puce , page 159
Obtention de certificats , page 98
Génération d'un fichier Keytab Kerberos , page 156
Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web d'iDRAC , page 140
Configuration d'Active Directory avec le schéma standard à l'aide de RACADM , page 141
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web iDRAC , page 151
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM , page 151

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 l'ouverture de session par carte à puce est activée, SSH, Telnet, IPMI sur le LAN, Serial over LAN (Série sur LAN) et l'interface distante RACADM sont désactivés. Notez de nouveau que si vous désactivez l'ouverture de session par carte à puce, les interfaces ne sont pas activées automatiquement.

Concepts associés

Obtention de certificats , page 98
Configuration de la connexion par carte à puce iDRAC pour les utilisateurs Active Directory , page 159
Configuration d'ouverture de session iDRAC par carte à puce pour les utilisateurs locaux , page 158

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 d'iDRAC, allez à **Présentation** > **Paramètres iDRAC** > **Authentification des utilisateurs** > **Carte à puce**.
   La page **Carte à puce** s'affiche.
2. Dans le menu déroulant **Configurer la connexion par carte à puce**, sélectionnez **Activé** pour activer l'ouverture de session par carte à puce ou **Activé avec l'interface RACADM distante**. Autrement, sélectionnez **Désactivé**.

   Pour plus d'informations sur les options, voir l'*Aide en ligne d'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 l’ouverture de session par carte à puce, utilisez la commande `set` avec des objets du groupe `iDRAC.SmartCard`.

Pour en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 la connexion par carte à puce. Autrement, sélectionnez **Désactivé**. Pour plus d'informations sur les options voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   La fonction d'ouverture de session par carte à puce est activée ou désactivée en fonction de votre sélection.

9

Configuration d'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 événement correspond à un filtre d'événement et que vous avez configuré ce filtre afin de générer une alerte (E-mail, Interruption SNMP, Alerte IPMI, Journaux système distant, Événements Redfish ou Événements 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 : L'activation des alertes SNMP via le système d'exploitation ou SNMP GET via le système d'exploitation hôte crée un utilisateur iDRAC *iSMnmpUser*.

Concepts associés

Activation ou désactivation des alertes , page 162
Filtrage des alertes , page 162
Définition d'alertes d'événement , page 163
Définition d'événement de récurrence d'alerte , page 164
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI , page 165
Configuration de la journalisation d'un système distant , page 176
Configuration des événements WS , page 168
Configuration des événements Redfish , page 169
ID de message d'alerte , page 170

Sujets :

- Activation ou désactivation des alertes
- Filtrage des alertes
- Définition d'alertes d'événement
- Définition d'événement de récurrence d'alerte
- Définition d'actions d'événement
- Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI
- Configuration des événements WS
- Configuration des événements Redfish
- Surveillance des événements de châssis
- ID de message d'alerte

Activation ou désactivation des alertes

Pour envoyer une alerte à des destinations définies ou exécuter une action d'événement, vous devez activer l'option d'alerte globale. Cette propriété remplace l'alerte individuelle ou les actions d'événement qui sont définies.

Concepts associés

Filtrage des alertes , page 162
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI , page 165

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 iDRAC, accédez à **Présentation** > **Serveur** > **Alertes**. La page **Alertes** s'affiche.
2. Dans la section **Alertes** :
   - Sélectionnez **Activer** pour activer la génération d'alertes ou exécuter une action d'événement.
   - Sélectionnez **Désactiver** pour désactiver la génération d'alerte ou une action d'événement.
3. Cliquez sur **Appliquer** pour enregistrer le paramètre.

Activation ou désactivation des alertes 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 iDRAC** s'affiche.
2. Dans **Événements de plate-forme**, sélectionnez **Activer** pour activer la génération d'alerte ou une action d'événement. Autrement, sélectionnez **Désactivé**. Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC.*
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres d'alerte sont définis.

Filtrage des alertes

Vous pouvez filtrer les alertes en fonction de la catégorie et de la gravité.

Concepts associés

Activation ou désactivation des alertes , page 162
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI , page 165

Filtrage des alertes à l'aide de l'interface Web iDRAC

Pour filtrer les alertes en fonction de la catégorie et de la gravité :

REMARQUE : Même si vous disposez de privilèges d'écriture uniquement, vous pouvez filtrer les alertes.

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Alertes**. La page **Alertes** s'affiche.
2. Dans la section **Filtre d'alertes** sélectionnez une ou plusieurs des catégories suivantes :
   - Intégrité du système
   - Stockage
   - Configuration
   - Audit
   - Mises à jour
   - Notes de travail
3. Sélectionnez un ou plusieurs des niveaux de gravité suivants :
   - Informatif
   - Avertissement
   - Critique
4. Cliquez sur **Appliquer**.
   La section **Résultats des alertes** affiche les résultats en fonction de la catégorie et de la gravité sélectionnées.

Filtrage des alertes à l'aide de l'interface RACADM

Pour filtrer les alertes, utilisez la commande **eventfilters**. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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.

Concepts associés

Activation ou désactivation des alertes , page 162
Configuration des paramètres d'alertes par e-mail, d'interruption SNMP ou d'interruption IPMI , page 165
Filtrage des alertes , page 162
Configuration de la journalisation d'un système distant , page 176
Configuration des événements WS , page 168
Configuration des événements Redfish , page 169

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. Allez sur **Présentation** > **Serveur** > **Alertes**.
   La page **Alertes** s'affiche.
3. Sous **Résultats d'alertes**, sélectionnez une alerte ou toutes les alertes suivantes des événements appropriés :
   - Alerte par e-mail
   - Interruption SNMP
   - Alerte IPMI
   - Journal système distant
   - Journal du SE
   - Événements WS
4. Cliquez sur **Appliquer**.
   Le paramétrage est enregistré.
5. Dans la section **Alertes**, sélectionnez **Activer** pour envoyer des alertes aux destinations définies.

6. Facultativement, vous pouvez envoyer un événement test. Dans le champ **ID de message pour tester l'événement**, saisissez l'ID de message pour tester si l'alerte est générée, puis cliquez sur **Tester**. Pour la liste des ID de message, voir le *Guide des messages d'événements* disponible à l'adresse **dell.com/support/manuals**.

Définition d'alertes d'événement à l'aide de l'interface RACADM

Pour définir une alerte d'événement, utilisez la commande **eventfilters**. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 Web iDRAC

Pour définir la valeur de récurrence d'alerte :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Alertes** > **Récurrence d'alerte**.
   La page **Récurrence d'alerte** s'affiche.
2. Dans la colonne **Récurrence**, entrez la valeur de fréquence d'alerte pour le ou les types de gravité, alerte et catégorie requis.
   Pour plus d'informations, voir l'*Aide en ligne d'iDRAC*.
3. Cliquez sur **Appliquer**.
   Les paramètres de récurrence d'alerte sont enregistrés.

Définition d'événements de récurrence d'alerte à l'aide de l'interface RACADM

Pour définir l'événement de récurrence d'alerte à l'aide de l'interface RACADM, utilisez la sous-commande **eventfilters**. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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.

Concepts associés

Filtrage des alertes , page 162
Activation ou désactivation des alertes , page 162

Définition d'actions d'événement à l'aide de l'interface Web

Pour configurer une action :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Alertes**. La page **Alertes** s'affiche.
2. Sous **Résultats d'alerte**, dans le menu déroulant **Actions** de chaque événement, sélectionnez une action :
   - Redémarrer
   - Cycle d'alimentation

- Mettre hors tension
- Aucune action

3. Cliquez sur **Appliquer**.
   Le paramétrage est enregistré.

Définition d'actions d'événements à l'aide de l'interface RACADM

Pour configurer une action d'événement, utilisez la commande `eventfilters`. Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 des données d'iDRAC. Pour les systèmes disposant de nombreux nœuds, il peut ne pas être efficace pour une station de gestion d'appeler chaque iDRAC pour chaque événement qui peut se produire. Par exemple, les interruptions d'événements peuvent aider une station de gestion avec l'équilibrage de charge entre les nœuds ou en émettant une alerte en cas d'échec de l'authentification. 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 également spécifier l'utilisateur SNMP v3 à qui 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.

Concepts associés

Configuration des destinations d'alerte IP , page 165
Configuration des paramètres d'alerte par e-mail , page 167

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 requis pour surveiller les serveurs à l'aide de SNMP, voir le *Guide de référence SNMP*, disponible sur **dell.com/support/manuals**.

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. Allez sous **Présentation** > **Serveur** > **Alertes** > **Paramètres SNMP et d'e-mail**.
2. Sélectionnez l'option **État** pour activer une destination d'alerte (adresse IPv4, adresse IPv6, ou Nom de domaine complet (FQDN)) pour recevoir les interruptions.
   Vous pouvez spécifier jusqu'à huit adresses de destination. Pour en savoir plus sur les options, voir l'*aide en ligne 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 de chaîne de communauté indique la chaîne de communauté à utiliser dans une alerte SNMP (Simple Network Management Protocol) envoyée par iDRAC. Veillez à ce que la chaîne de communauté de destination soit identique à la chaîne de communauté 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 de l'e-mail. Les valeurs autorisées vont de 1 à 8.
<n>=0 **<n>**=1	Désactiver l'interruption Activer l'interruption

2. Pour définir l'adresse de destination de l'interruption :

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

Paramètre	Description
<index>	Index de destination de l'e-mail. Les valeurs autorisées vont de 1 à 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 des 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 en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration des adresses de destination d'alerte IP à l'aide de l'utilitaire de configuration d'iDRAC

Vous pouvez configurer les destinations d'alerte (IPv4, IPv6, ou FQDN) à l'aide de l'utilitaire Paramètres iDRAC. Pour ce faire :

1. Dans l'**utilitaire de configuration d'iDRAC**, accédez à **Alertes**.
   La page **Paramètres d'alerte d'iDRAC** s'affiche.
2. Sous **Paramètres d'interruption**, activez la ou les adresses IP pour recevoir les interruptions et entrez la ou les adresses IPv4, IPv6, ou FQDN de destination. Vous pouvez définir jusqu'à huit adresses.
3. Entrez le nom de la chaîne de communauté.

   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
4. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les destinations d'alerte sont configurées.

Configuration des paramètres d'alerte par e-mail

Vous pouvez configurer l'adresse e-mail destinataire des alertes par e-mail. Configurez également les paramètres d'adresse du serveur SMTP.

REMARQUE : Si vous utilisez le serveur de messagerie Microsoft Exchange Server 2007, veillez à ce que le nom de domaine d'iDRAC soit configuré pour que le serveur de messagerie puisse recevoir les alertes par e-mail d'iDRAC.

REMARQUE : Les alertes par e-mail prennent en charge les adresses iPv4 et IPv6. Le nom de domaine DNS DRAC doit être défini lorsque vous utilisez IPv6.

Concepts associés

Configuration des paramètres de l'adresse du serveur de messagerie SMTP , page 168

Configuration des paramètres des alertes par e-mail à l'aide de l'interface Web :

Pour configurer les paramètres d'alerte par e-mail en utilisant l'interface Web :

1. Allez sous **Présentation** > **Serveur** > **Alertes** > **Paramètres SNMP et e-mail**.
2. Sélectionnez l'option **État** pour activer l'adresse e-mail pour recevoir des alertes et tapez une adresse e-mail valide. Pour plus d'informations sur les options, voir l'*aide en ligne d'iDRAC.*
3. Cliquez sur **Envoyer** sous **E-mail test** pour tester les paramètres des alertes par e-mail.
4. Cliquez sur **Appliquer**.

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 de l'e-mail. Les valeurs autorisées vont de 1 à 4.
n=0 **n**=1	Désactive les alertes par e-mail. 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 de l'e-mail. Les valeurs autorisées vont de 1 à 4.
email-address	Adresse e-mail de destination qui reçoit les alertes d'événements de la plate-forme.

3. Pour configurer un message personnalisé :

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

Paramètre	Description
index	Index de destination de l'e-mail. Les valeurs autorisées vont de 1 à 4.
custom-message	Message personnalisé

4. 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 vont de 1 à 4.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 iDRAC

Pour définir l'adresse du serveur SMTP :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Alertes** > **Paramètres SNMP et de messagerie**.
2. Entrez l'adresse IP valide ou le nom de domaine pleinement qualifié (FQDN) du serveur SMTP à utiliser au cours de la configuration.
3. Sélectionnez l'option **Activer l'authentification**, puis entrez le nom d'utilisateur et le mot de passe d'un utilisateur qui a accès au serveur SMTP.
4. Entrez le numéro de port SMTP.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'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 WS

Le protocole des événements WS est utilisé pour un service client (abonné) pour enregistrer l'intérêt (abonnement) sur un serveur (source d'événement) pour recevoir les messages contenant les événements de serveur (notifications ou messages d'événement). Les clients souhaitant recevoir des messages d'événement WS peuvent s'inscrire à iDRAC et recevoir des événements de tâche du Lifecycle Controller.

Les étapes requises pour configurer la fonction des événements WS afin de recevoir les messages d'événements WS relatifs aux tâches du Lifecycle Controller sont décrites dans le document de spécifications Web service Eventing Support for iDRAC 1.30.30 (Prise en charge des événements Web Service pour iDRAC7 1.30.30). Outre ce document, consultez le document DSP0226 [DMTF WS Management Specification (Spécification de gestion WS DMTF)], notifications de section 10 [Eventing (Événements)] pour des informations exhaustives concernant le protocole des événements WS. Les tâches relatives au Lifecycle Controller sont décrites dans le document DCIM Job Control Profile (Profil du contrôle des tâches DCIM).

Configuration des événements Redfish

Le protocole des événements Redfish est utilisé pour un service client (abonné) pour enregistrer l'intérêt (abonnement) sur un serveur (source d'événement) pour recevoir les messages contenant les événements Redfish (notifications ou messages d'événement). Les clients souhaitant recevoir des messages d'événement Redfish peuvent s'inscrire à iDRAC et recevoir des événements de tâche du Lifecycle Controller.

Surveillance des événements de châssis

Sur le châssis PowerEdge FX2/FX2s, vous pouvez activer le paramètre **Gestion et surveillance du châssis** dans iDRAC pour effectuer des tâches de gestion et de surveillance du châssis, telles que la surveillance des composants du châssis, la configuration des alertes, l'utilisation d'iDRAC RACADM pour transmettre des commandes RACADM CMC et la mise à jour du firmware de gestion du châssis. Ce paramètre vous permet de gérer les serveurs dans le châssis, même si CMC n'est pas sur le réseau. Vous pouvez définir la valeur sur **Désactivé** pour transférer les événements du châssis. Par défaut, ce paramètre est défini sur **Activé**.

REMARQUE : Pour que ce paramètre prenne effet, vous devez vous assurer que dans le CMC, l'option **Gestion du châssis en mode Serveur** est définie sur **Écran** ou **Gérer et surveiller**.

Lorsque l'option **Gestion et surveillance du châssis** est définie sur **Activé**, iDRAC génère et enregistre les événements du châssis. Les événements générés sont intégrés dans le sous-système d'événements iDRAC et des alertes sont générées de la même manière que les autres événements.

CMC transfère également les événements générés à iDRAC. Si iDRAC ne fonctionne pas sur le serveur, CMC met en file d'attente les 16 premiers événements et consigne le reste dans le journal de CMC. Ces 16 événements sont envoyés à iDRAC dès que l'option **Surveillance du châssis** est définie sur Activé.

Lorsque l'iDRAC détecte qu'une fonctionnalité CMC requise est absente, un message d'avertissement s'affiche pour vous informer que certaines fonctionnalités risquent de ne plus être fonctionnelles sans une mise à niveau du micrologiciel du CMC.

Surveillance des événements du châssis à l'aide de l'interface Web iDRAC

Pour surveiller les événements du châssis à l'aide de l'interface Web iDRAC, effectuez les opérations suivantes :

REMARQUE : Cette section s'affiche uniquement pour des châssis PowerEdge FX2/FX2s et si le mode de **Gestion du châssis basé sur le serveur** est défini sur **Écran** ou **Gérer et surveiller** dans le CMC.

1. Sur l'interface CMC, cliquez sur **Présentation du châssis** > **Configuration** > **Généralités**.
2. Depuis le menu déroulant **Gestion du châssis en mode serveur**, sélectionnez **Gérer et surveiller**, puis cliquez sur **Appliquer**.
3. Lancement de l'interface Web iDRAC, cliquez sur **Présentation** > **Paramètres iDRAC** > **CMC**.
4. Sous la section **Gestion du châssis basé sur le serveur**, assurez-vous que la zone de liste déroulante **Fonctionnalité d'iDRAC** est définie sur **Activé**.

Surveillance des événements du châssis à l'aide de RACADM

Ce paramètre s'applique uniquement aux serveurs PowerEdge FX2/FX2s et si le mode de **gestion du châssis basé sur le serveur** est défini sur **Écran** ou **Gérer et surveiller** dans le CMC.

Pour surveiller les événements du châssis iDRAC à l'aide de RACADM iDRAC :

```
racadm get system.chassiscontrol.chassismanagementmonitoring
```

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

ID de message d'alerte

Le tableau suivant répertorie les ID de message affichés pour les alertes.

Tableau 29. ID de message d'alerte

ID du message	Description
AMP	Ampérage
ASR	Réinitialisation automatique du système
BAR	Sauvegarde/Restauration
BAT	Événement de batterie
BIOS	Gestion du BIOS
BOOT	Contrôle de l'amorçage
CBL	Câble
UC	Processeur
CPUA	Proc absent
CTL	Contrôle stockage
DH	Gestion cert
DIS	Détection automatique
ENC	Enceinte stockage
FAN	Événement ventilateur
FSD	Débogage
HWC	Configuration matérielle
IPA	Changement d'adresse IP DRAC
ITR	Intrusion
JCP	Contrôle des tâches
LC	Lifecycle Controller
LIC	Licences
LNK	Condition de la liaison
LOG	Événement journal
MEM	Mémoire
NDR	Pilote SE NIC

Tableau 29. ID de message d'alerte (suite)

ID du message	Description
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
RED	Téléchargement FW
RFL	Média IDSDM
RFLA	IDSDM Absent
RFM	SD FlexAddress
RRDU	Redondance IDSDM
RSI	Service à distance
SEC	Événement sécurité
Journal d'évènements système	Journal des événements système
SRD	RAID logiciel
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

Tableau 29. ID de message d'alerte (suite)

ID du message	Description
UEFI	Événement UEFI
USR	Suivi utilisateur
VDR	Disque virtuel
VF	Une carte SD vFlash
VFL	Événement vFlash
VFLA	vFlash absent
VLT	Tension
VME	Média virtuel
VRM	Console virtuelle
WRK	Note de travail

10

Gestion des journaux

IDRAC fournit un journal Lifecycle qui contient les événements associés aux systèmes, périphériques de stockage, périphériques de réseau, mises à jour du micrologiciel, 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 d'iDRAC, RACADM et WSMAN.

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.

Concepts associés

Affichage du journal des événements système , page 173
Affichage du journal Lifecycle , page 174
Exportation des journaux du Lifecycle Controller , page 175
Ajout de notes de travail , page 176
Configuration de la journalisation d'un système distant , page 176

Sujets :

- Affichage du journal des événements système
- Affichage du journal Lifecycle
- Exportation des journaux du Lifecycle Controller
- Ajout de notes de travail
- Configuration de la journalisation d'un système distant

Affichage du journal des événements système

Lorsqu'un événement se produit sur un système géré, il est enregistré dans le journal SEL (System Event Log). La même entrée SEL est disponible dans le journal LC.

Affichage du journal des événements système à l'aide de l'interface Web

Pour afficher le journal SEL, dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Journaux**.

La page du **System Event Log (Journal des événements système)** affiche un indicateur d'intégrité du système, un horodatage et la description de chaque événement journalisé. Pour plus d'informations, voir l'*Aide en ligne d'iDRAC*.

Cliquez sur **Enregistrer sous** pour enregistrer le journal **SEL** dans le répertoire de votre choix.

REMARQUE : Si vous utilisez Internet Explorer et si vous rencontrez un problème lors de l'enregistrement, téléchargez la mise à jour de sécurité cumulative pour Internet Explorer. Vous pouvez la télécharger à partir du site Web de support de Microsoft à l'adresse **support.microsoft.com**.

Pour effacer les journaux, cliquez sur **Effacer le journal**.

REMARQUE : Le bouton **Effacer le journal** n'apparaît que si vous disposez de l'autorisation Effacer les journaux.

Une fois que le journal SEL est effacé, une entrée est consignée dans le journal du Lifecycle Controller. L'entrée de journal inclut le nom d'utilisateur et l'adresse IP de l'emplacement où le journal SEL a été effacé.

Affichage du journal des événements système à l'aide de l'interface RACADM

Pour afficher le journal SEL :

```
racadm getsel <options>
```

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

Pour afficher le nombre d'entrées du journal SEL : `racadm getsel -i`

Pour effacer les entrées du journal SEL : `racadm clrsel`

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 Paramètres iDRAC. Pour ce faire :

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 **Oui**. Sinon, sélectionnez **Non**.
3. Pour afficher les événements système, cliquez sur **Affichage du journal d'événements du système**.
4. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.

Affichage du journal Lifecycle

Les journaux Lifecycle Controller contiennent l'historique des modifications associées aux composants installés sur un système géré. Vous pouvez également ajouter des notes de travail pour chaque entrée de journal.

Les événements et les activités suivantes sont consignés :

- Système
- Périphériques de stockage
- Périphériques réseau
- Configuration
- Audit
- Mises à jour

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 d'ouverture de session sont consignés dans les journaux Lifecycle :

- Telnet
- SSH
- Interface web
- RACADM
- SM-CLP
- IPMI sur le LAN
- Série
- Console virtuelle
- Média virtuel

Vous pouvez afficher et filtrer les journaux en fonction de la catégorie et du niveau de gravité. Vous pouvez également exporter et ajouter une note de travail 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.

Tâches associées

Filtrage des journaux Lifecycle , page 175
Exportation des journaux du Lifecycle Controller à l'aide de l'interface Web , page 175
Ajout de commentaires aux journaux Lifecycle , page 175

Affichage du journal Lifecycle à l'aide de l'interface Web

Pour afficher les journaux Lifecycle, cliquez sur **Présentation** > **Serveur** > **Journaux** > **Journal Lifecycle**. La page **Journal Lifecycle** s'affiche. Pour en savoir plus, 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 du journal filtré 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 afficher les journaux Lifecycle, utilisez la commande `lclog`.

Pour en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Exportation des journaux du Lifecycle Controller

Vous pouvez exporter le journal du Lifecycle Controller entier (entrées actives et archivées) dans un seul fichier compressé XML sur un partage réseau ou sur le système local. L'extension de fichier XML compacté est `.xml.gz`. Les entrées de fichier sont commandées de façon séquentielle en fonction de leurs numéros de séquence, commandées à partir du numéro de séquence le plus bas jusqu'au plus élevé.

Exportation des journaux du Lifecycle Controller 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 vers un emplacement partagé du réseau.
   - **Local** : exportez les journaux Lifecycle vers un emplacement sur le système local.

REMARQUE : Lorsque vous indiquez les paramètres de partage du 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 d'iDRAC*.

3. Cliquez sur **Exporter** pour exporter le journal sur un emplacement spécifié.

   REMARQUE : L'iDRAC ne peut pas accéder à un partage CIFS si toutes les conditions suivantes sont remplies :
   - Le partage CIFS Windows est situé sur un domaine.
   - Le protocole SMB2 est activé et l'authentification LAN Manager est définie sur *Send NTLMv2 response only (Envoyer uniquement la réponse NTLMv2). Refuse LM & NTLM (Refuser LM & NTLM)*.

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 référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/support/manuals**.

Ajout de notes de travail

Chaque utilisateur qui ouvre une session sur iDRAC peut ajouter des notes de travail qui sont stockées dans le journal Lifecycle sous la forme d'un événement. Vous devez disposer du privilège Journaux iDRAC pour pouvoir ajouter des notes de travail. Chaque note peut contenir jusqu'à 255 caractères.

REMARQUE : Vous ne pouvez pas supprimer une note de travail.

Pour ajouter une note de travail :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Propriétés** > **Récapitulatif**.
   La page du **Résumé du système** s'affiche.
2. Dans **Notes de travail**, entrez le texte dans la zone de texte vide.

   REMARQUE : Il est recommandé de ne pas utiliser un trop grand nombre de caractères spéciaux.

3. Cliquez sur **Add** (Ajouter).
   La note de travail est ajoutée au journal. Pour en savoir plus, voir l'*Aide en ligne d'iDRAC*.

Configuration de la journalisation d'un système distant

Vous pouvez envoyer des journaux Lifecycle à un système distant. Auparavant, vérifiez que :
- Il existe une connectivité réseau entre iDRAC et le système distant.
- Le système distant et iDRAC se trouvent dans le même réseau.

Configuration de la journalisation d'un système distant à l'aide de l'interface Web

Pour configurer les paramètres d'un serveur syslog distant :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Journaux** > **Paramètres**.
   L'écran **Paramètres du syslog distant** s'affiche.
2. Activez le serveur syslog distant, définissez l'adresse du serveur et spécifiez le numéro de port. Pour plus d'informations sur les options, voir l'*Aide en ligne d'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 journalisation d'un système distant, utilisez la commande `set` avec les objets du groupe `iDRAC.SysLog`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

11

Surveillance et gestion de l'alimentation

Vous pouvez utiliser iDRAC pour surveiller et gérer l'alimentation du système géré afin de protéger le système contre les surtensions en distribuant et en régulant de manière appropriée la consommation d'alimentation du système.

Les principales fonctions sont les suivantes :

- **Surveillance de l'alimentation** : affichage de l'état de l'alimentation, historique des mesures d'alimentation, moyennes de courant, pics, etc. associés au système géré.
- **Limitation de la puissance :** affichage et définition de la limitation de puissance du système géré, y compris l'affichage de la consommation électrique potentielle maximale et minimale. Il s'agit d'une fonction disponible sous licence.
- **Contrôle de l'alimentation :** exécution à distance d'opérations de contrôle de l'alimentation (mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation et arrêt normal) sur le système géré.
- **Options d'alimentation** : configuration des options d'alimentation, telles que stratégie de redondance, disque de secours et correction du facteur de puissance.

Concepts associés

Surveillance de l'alimentation , page 178
Exécution d'opérations de contrôle de l'alimentation , page 179
Plafonnement de l'alimentation , page 180
Configuration des options d'alimentation , page 181
Activation ou désactivation du bouton d'alimentation , page 183
Définition du seuil d'avertissement de consommation d'alimentation , page 179

Sujets :

- Surveillance de l'alimentation
- Définition du seuil d'avertissement de consommation d'alimentation
- Exécution d'opérations de contrôle de l'alimentation
- Plafonnement de l'alimentation
- Configuration des options d'alimentation
- Activation ou désactivation du bouton d'alimentation

Surveillance de l'alimentation

iDRAC surveille la consommation d'alimentation du système en continu et affiche les valeurs d'alimentation suivantes :

- Seuils d'avertissement de consommation d'énergie et critiques.
- Valeurs de puissance cumulée, de puissance de crête et pic d'intensité de courant électrique.
- Consommation d'énergie au cours de la dernière heure, du dernier jour ou de la dernière semaine.
- Consommation d'énergie moyenne, minimale et maximale
- Historique des pics et horodatage des pics.
- Pic de marge de sécurité et valeurs de marge de sécurité instantanée (pour les serveurs en rack et de type tour).

REMARQUE : L'histogramme représentant la tendance de consommation de puissance du système (toutes les heures, tous les jours, toutes les semaines) est uniquement conservée pendant que l'iDRAC est en cours d'exécution. Si l'iDRAC redémarre, les données de consommation électrique existantes sont perdues et l'histogramme est redémarré.

Surveillance de l'alimentation à l'aide de l'interface Web

Pour afficher les informations de surveillance de l'alimentation, dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation/Thermique** > **Surveillance de l'alimentation**. La page **Surveillance de l'alimentation** s'affiche. Pour en savoir plus, voir l'*Aide en ligne d'iDRAC*.

Surveillance de l’alimentation à l’aide de RACADM

Pour afficher les informations de surveillance de l’alimentation, utilisez la commande `get` avec les objets du groupe `System.Power`.

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 seuil d’avertissement de consommation d'alimentation

Vous pouvez définir la valeur du seuil d’avertissement du capteur de consommation d’alimentation dans les systèmes en rack ou en tour. Le seuil d’alimentation d’avertissement/critique pour les serveurs en rack et en tour peut changer lors du cycle d’alimentation du système selon la capacité du PSU (Power Supply Unit, Unité d’alimentation) 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.

Le seuil d’avertissement d’alimentation des systèmes lame est défini sur l'attribution d'alimentation CMC.

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 d’alimentation.

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 d'énergie à l’aide de l’interface Web

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation / Thermique** > **Surveillance d'alimentation**. La page **Surveillance de l'alimentation** s'affiche.
2. Dans la section **Seuils et mesures d'alimentation actuels**, dans la colonne **Seuil d’avertissement**, saisissez la valeur en **Watts** ou **en BTU/h**.

   Les valeurs doivent être inférieures à celles des valeurs du **Seuil de panne**. 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 en **BTU/h**. De la même façon, si vous entrez BTU/h, la valeur en **Watts** s’affiche.
3. Cliquez sur **Appliquer**. Les valeurs sont configurées.

Exécution d’opérations de contrôle de l’alimentation

iDRAC permet d’exécuter à distance une mise sous tension, une mise hors tension, une réinitialisation, un arrêt normal, une interruption NMI (Non-Masking Interrupt) ou un cycle d’alimentation à l’aide de l’interface web ou RACADM.

Vous pouvez également exécuter ces opérations à l’aide des services à distance Lifecycle Controller ou WSMAN. Pour plus d'informations, voir le *Lifecycle Controller Remote Services Quick Start Guide* (Guide de démarrage rapide des services à distance de Lifecycle Controller) disponible sur **dell.com/idracmanuals** et le document de profil *Dell Power State Management* (Gestion de l'état de l'alimentation Dell) disponible à l'adresse **delltechcenter.com**.

Les opérations de commande à distance de l’alimentation initiées à partir d’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 iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation/Thermique** > **Configuration de l'alimentation** > **Contrôle de l'alimentation**. La page **Contrôle de l'alimentation** s'affiche.

2. Sélectionnez l'opération d'alimentation appropriée :
   - Mettre le système sous tension
   - Arrêter le système
   - NMI (interruption non masquable)
   - Arrêt normal
   - Réinitialiser le système (démarrage à chaud)
   - Exécuter un cycle d'alimentation du système (démarrage à froid)
3. Cliquez sur **Appliquer**. Pour en savoir plus, voir l'*aide en ligne d'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 en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Plafonnement de l'alimentation

Vous pouvez afficher les limites de seuil de puissance qui couvrent la plage de consommation électrique CA et CC qu'un système soumis à une forte charge de travail présente au centre de données. Cette fonction est disponible sous licence.

Limitation de la puissance dans les serveurs lames

Avant la mise sous tension d'un serveur lame dans un châssis PowerEdge M1000e ou PowerEdge VRTX, l'iDRAC fournit à CMC l'alimentation nécessaire. Cette quantité d'alimentation est plus élevée que la quantité d'alimentation réelle que le serveur lame peut consommer et est calculée en fonction d'informations d'inventaire matériel limitées. Il peut demander une plage d'alimentation plus petite après la mise sous tension du serveur en fonction de l'alimentation réelle consommée par le serveur. Si la consommation d'alimentation augmente au fil du temps et que le serveur atteint presque sa consommation d'alimentation maximale, l'iDRAC peut demander une augmentation de la consommation d'alimentation potentielle maximale, ce qui augmente l'enveloppe d'alimentation. L'iDRAC augmente uniquement sa demande de consommation d'alimentation potentielle maximale au CMC. Il ne demande pas une alimentation minimale potentielle inférieure si la consommation diminue. L'iDRAC continue à demander plus de puissance si la consommation d'alimentation dépasse l'alimentation allouée par le CMC.

Une fois le système sous tension et initialisé, iDRAC calcule une nouvelle exigence d'alimentation en fonction de la configuration de la lame. La lame reste sous tension, même si CMC ne parvient pas à satisfaire la nouvelle demande d'alimentation.

Le CMC récupère toute la puissance non utilisée des serveurs à priorité inférieure et alloue ensuite cette puissance récupérée à un module d'infrastructure ou un serveur à priorité supérieure.

Si l'alimentation allouée est insuffisante, le serveur lame n'est pas mis sous tension. Si la lame reçoit une alimentation suffisante, iDRAC met le système sous tension.

Affichage et configuration d'une stratégie de limitation de puissance

Lorsqu'une stratégie appropriée de limitation de puissance est activée, elle applique les limites de puissance définies par l'utilisateur au système. Si la stratégie n'est pas activée, elle utilise la stratégie de protection de la puissance du matériel mise en œuvre par défaut. Cette stratégie de protection de puissance est indépendant de la stratégie définie par l'utilisateur. Les performances du système sont ajustées dynamiquement pour maintenir la consommation électrique proche du seuil défini.

La consommation électrique réelle peut être inférieure pour les faibles charges de travail et peut dépasser temporairement le seuil jusqu'à l'ajustement des performances. Par exemple, pour une configuration système donnée, la consommation électrique potentielle maximale est de 700 W et la consommation électrique potentielle moyenne est de 500 W. Vous pouvez définir et activer un seuil de budget énergétique pour faire passer la consommation de 650 W à 525 W. À partir de là, les performances du système sont ajustées dynamiquement pour maintenir la consommation électrique pour ne pas dépasser le seuil de 525 W défini par l'utilisateur.

Si la valeur de limite d'alimentation est inférieure au seuil minimal recommandé, iDRAC ne peut pas maintenir la limite d'alimentation demandée.

Vous pouvez définir la valeur en watts, BTU/h ou sous la forme d'un pourcentage (%) de la limite de puissance maximale recommandée.

Lorsque vous définissez le seuil de limite de puissance en BTU/h, la conversion en watts est arrondie à l'entier le plus proche. Lors de la lecture du seuil de limite de puissance, la conversion des watts en BTU/h est de nouveau arrondie de cette manière. Par conséquent, la valeur écrite peut être nominalement différente de la valeur lue. Par exemple, la lecture du seuil de 600 BTU/h donne 601 BTU/h.

Configuration d'une stratégie de limitation de puissance à l'aide de l'interface Web

Pour afficher et configurer des stratégies d'alimentation :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Alimentation/Thermique** > **Configuration de l'alimentation** > **Configuration de l'alimentation**. La page **Configuration de l'alimentation** s'affiche.
   La page **Configuration de l'alimentation** s'affiche. La limite de la stratégie d'alimentation actuelle figure dans la section **Stratégie de limite d'alimentation active**.
2. Sélectionnez **Activer** sous **Stratégie de limite d'alimentation iDRAC**.
3. Dans la section **Limites définies par l'utilisateur**, entrez la limite de puissance maximale en watts et en BTU/h ou le pourcentage maximal de limite système recommandée.
4. Cliquez sur **Appliquer** pour appliquer les valeurs.

Configuration d'une stratégie de limitation de l'alimentation à l'aide de l'interface RACADM

Pour afficher et définir les valeurs actuelles de limitation de l'alimentation, utilisez les objets suivants avec la commande `set` :

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 l'unité d'alimentation du serveur prend en charge la surveillance de l'alimentation.

   La page **Paramètres iDRAC - Configuration de l'alimentation** s'affiche.
2. Sélectionnez **Activé** pour activer la **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 composant d'échange à chaud et la correction de facteur de puissance.

Le disque de secours est une fonction d'alimentation qui configure les unités d'alimentation pour qu'elles se mettent hors tension en fonction de la charge du serveur. Ceci permet aux unités d'alimentation restantes de fonctionner avec une charge plus élevée et plus efficacement. Pour cela, il est nécessaire que les unités d'alimentation prennent en charge cette fonction pour qu'elles se mettent sous tension rapidement lorsque cela est nécessaire.

Dans un système à deux UC, l'UC1 ou UC2 peut être configurée en tant qu'UC principale. Dans un système à quatre UC, vous devez définir la paire d'UC (1+1 ou 2+2) en tant qu'UC principale.

Une fois le disque de secours activé, les unités d'alimentation peuvent devenir actives ou se mettre en veille en fonction de la charge. Si le disque de secours est activé, le partage de courant électrique asymétrique entre les deux unités d'alimentation est activé. Une unité d'alimentation est *allumée* et fournit la majorité du courant ; l'autre unité est en mode veille et fournit une petite quantité de courant. Cette configuration de deux unités d'alimentation et d'un disque de secours activés est souvent appelée 1+0. Si toutes les unités d'alimentation 1 se trouvent sur le circuit A et que toutes les unités d'alimentation 2 se trouvent sur le circuit B, ce dernier a beaucoup moins de charge et déclenche les avertissements avec le disque de secours est activé (configuration d'usine du disque de secours par défaut). Si le disque de secours est désactivé, le courant électrique est partagé à 50/50 entre les deux unités d'alimentation, le circuit A et le circuit B ayant normalement la même charge.

Le facteur de puissance est le rapport de l'alimentation réelle consommée et de l'alimentation apparente. Lorsque la correction du facteur de puissance est activée, le serveur consomme une petite quantité d'alimentation lorsque l'hôte est désactivé. Par défaut, la correction du facteur d'alimentation est activée lorsque le serveur est expédié de l'usine.

Configuration des options d'alimentation à l'aide de l'interface Web

Pour configurer les options d'alimentation :

1. Dans l'interface Web d'iDRAC accédez à **Présentation** > **Serveur** > **Alimentation/Thermique** > **Configuration de l'alimentation** > **Configuration de l'alimentation**. La page **Configuration de l'alimentation** s'affiche.
2. Sous **Options d'alimentation**, sélectionnez les options appropriées. Pour en savoir plus, voir l'*Aide en ligne d'iDRAC*.
3. Cliquez sur **Appliquer**. Les options d'alimentation sont configurées.

Configuration des options d'alimentation électrique à l'aide de l'interface RACADM

Pour configurer les options d'alimentation électrique, utilisez les objets suivants avec la sous-commande `set` :

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration des options d'alimentation à l'aide de l'utilitaire de configuration d'iDRAC

Pour configurer les options d'alimentation :

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

   REMARQUE : Le lien **Configuration de l'alimentation** est disponible uniquement si l'unité d'alimentation du serveur prend en charge la surveillance de l'alimentation.

   La page **Paramètres iDRAC - Configuration de l'alimentation** s'affiche.
2. Dans les **options d'alimentation** :
   - Activez ou désactivez la redondance d'alimentation.
   - Activez ou désactivez le composant de secours.
   - Définissez l'unité d'alimentation principale.
   - Activez ou désactivez la correction de facteur de puissance. Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les options d'alimentation sont définies.

Activation ou désactivation du bouton 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.

12

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)
- Cartes NCD (Network Daughter Card)
- Cartes mezzanines (uniquement pour les serveurs lames)

Avant de désactiver NPAR ou une partition individuelle sur des périphériques CNA, assurez-vous que vous effacez 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 la bande passante). Vous pouvez désactiver une partition par la modification du paramètre d'attribut VirtualizationMode sur NPAR ou par la désactivation de toutes les personnalités sur une partition.

Selon le type de périphérique CNA installé, les paramètres des attributs de partition peuvent ne pas être conservés à partir de la dernière fois que la partition a été active. Configurez tous les attributs d'identité d'E/S et relatifs à la partition lors de l'activation d'une partition. Vous pouvez activer une partition par la modification du paramètre d'attribut VirtualizationMode sur NPAR ou par l'activation d'une personnalité (par exemple : NicMode) sur la partition.

Concepts associés

Inventaire et surveillance des périphériques HBA FC , page 185
Configuration dynamique des adresses virtuelles, de l'initiateur et de la cible de stockage , page 185

Sujets :

- Inventaire et surveillance des périphériques réseau
- Inventaire et surveillance des périphériques HBA FC
- Configuration dynamique des adresses virtuelles, de l'initiateur et de la cible de stockage

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 capacités
- Statistiques de réception et de transmission
- iSCSI, initiateur FCoE et informations de la cible

Concepts associés

Configuration, surveillance et inventaire des périphériques réseau , page 184
Configuration dynamique des adresses virtuelles, de l'initiateur et de la cible de stockage , page 185

Surveillance des périphériques réseau à l'aide de l'interface Web

Pour afficher les informations des périphériques réseau à l'aide de l'interface Web, accédez à **Présentation** > **Matériel** > **Périphériques réseau**. La page **Périphériques réseau** s'affiche. Pour plus d'informations sur les propriétés affichées, voir l'*Aide en ligne d'iDRAC*.

REMARQUE : Si l'**État des pilotes SE** signale qu'ils sont opérationnels, il indique l'état de pilotes du système d'exploitation ou d'UEFI

Surveillance des périphériques réseau à l'aide de RACADM

Pour afficher des informations sur les périphériques réseau, utilisez les commandes `hwinventory` et `nicstatistics`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

D'autres propriétés peuvent s'afficher lors de l'utilisation de RACADM ou de WSMAN en plus des propriétés affichées dans l'interface web iDRAC.

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 et état des liaisons
- Propriétés du port
- Statistiques de réception et de transmission

Concepts associés

Configuration, surveillance et inventaire des périphériques réseau , page 184

Surveillance des périphériques HBA FC à l'aide de l'interface Web

Pour afficher les informations sur les périphériques HBA FC à l'aide de l'interface Web, allez à **Présentation** > **Matériel** > **Fibre Channel**. Pour en savoir plus sur les propriétés affichées, voir l'*Aide en ligne 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.

Surveillance des périphériques HBA FC à l'aide de RACADM

Pour afficher les informations des périphériques HBA FC à l'aide de RACADM, utilisez la commande `hwinventory`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration dynamique des adresses virtuelles, de l'initiateur et de la cible de stockage

Vous pouvez afficher une vue dynamique et configurer les paramètres d'adresse virtuelle, de l'initiateur et de la cible de stockage, et appliquer une règle de persistance. Celle-ci permet à l'application d'appliquer les paramètres en fonction des changements d'état de l'alimentation (redémarrage du système d'exploitation, redémarrage à chaud, redémarrage à froid ou cycle CA) et en fonction de la configuration de la règle de persistance pour cet état d'alimentation. Cela permet une flexibilité accrue dans les déploiements pour lesquels les charges de travail du système doivent être rapidement reconfigurées sur 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 du traitement de l'alimentation principale au cours de la réinitialisation du système et si la NIC, le CNA ou le HBA dispose d'une alimentation auxiliaire. La persistance des paramètres de l'identité d'E/S peut être obtenue en fonction de la configuration de la règle effectuée à l'aide d'iDRAC.

Les règles de persistance prennent effet uniquement si la fonction d'identité d'E/S est activée. Chaque fois que le système redémarre ou est mis sous tension, les valeurs sont conservées ou effacées en fonction des paramètres de la règle.

REMARQUE : Une fois les valeurs effacées, vous ne pouvez pas les ré-appliquer avant d'exécuter la tâche de configuration.

Concepts associés

Configuration, surveillance et inventaire des périphériques réseau , page 184
Cartes prises en charge pour l'optimisation d'identité d'E/S , page 186
Versions du micrologiciel des cartes réseau prises en charge pour l'optimisation de l'identité des E/S , page 187
Activation ou désactivation de l'optimisation d'identité d'E/S , page 189
Configuration des paramètres de la stratégie de persistance , page 190

Cartes prises en charge pour l'optimisation d'identité d'E/S

Le tableau suivant indique les cartes qui prennent en charge la fonction d'optimisation d'identité d'E/S.

Tableau 30. Cartes prises en charge pour l'optimisation d'identité d'E/S

Fabricant	Type
Broadcom	• 5720 PCIe 1 Go • 5719 PCIe 1 Go • 57810 PCIe 10 Go • 57810 bNDC 10 Go • 57800 rNDC 10 Go + 1 Go • 57840 rNDC 10 Go • 57840 bNDC 10 Go • 5720 rNDC 1 Go • 5719 Mezz 1 Go • 57810 Mezz 10 Go • 5720 bNDC 1 Go
Intel	• i350 Mezz 1 Gbit • x520+i350 rNDC 10 Gbit+1 Gbit • I350 bNDC 1 Gbit • x540 PCIe 10 Gbit • x520 PCIe 10 Gbit • i350 PCIe 1 Gbit • x540+i350 rNDC 10 Gbit+1 Gbit • i350 rNDC 1 Gbit • x520 bNDC 10 Gbit • 40G 2P XL710 rNDC QSFP+
Mellanox	• ConnectX-3 10G • ConnectX-3 40G • ConnectX-3 10G • ConnectX-3 Pro 10G • ConnectX-3 Pro 40G • ConnectX-3 Pro 10G

Tableau 30. Cartes prises en charge pour l'optimisation d'identité d'E/S (suite)

Fabricant	Type
QLogic	• QME2662 Mezz FC16 • QLE2660 PCIe FC16 • QLE2662 PCIe FC16
Emulex	• LPM16002 Mezz FC16 • LPe16000 PCIe FC16 • LPe16002 PCIe FC16 • LPM16002 Mezz FC16 • LPM15002 • LPe15000 • LPe15002 • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104-UX-D rNDC 10 Gbit • OCm14102-U2-D bNDC 10 Gbit • OCm14102-U3-D Mezz 10 Gbit • OCe14102-UX-D PCIe 10 Gbit

Versions du micrologiciel des cartes réseau prises en charge pour l'optimisation de l'identité des E/S

Dans les serveurs de 13e génération Dell PowerEdge, le micrologiciel de carte NIC nécessaire est disponible par défaut.

Le tableau suivant indique les versions du micrologiciel de la carte réseau pour la fonctionnalité d'optimisation d'identité d'E/S.

Comportement de Virtual ou Flex Address et de la stratégie de persistance lorsque le contrôleur iDRAC est défini sur le mode Console ou Flex Address

Le tableau suivant décrit le comportement de la stratégie Virtual Address Management (Gestion des adresses virtuelles) et le comportement de la stratégie de persistance en fonction de l'état de la fonction Flex Address dans le CMC, mode défini dans l'iDRAC, de l'identité d'E/S dans l'iDRAC et l'état de la fonction de configuration XML.

Tableau 31. Comportement de Virtual/Flex Address et de la stratégie de persistance

État de la fonction FlexAddress dans le CMC	Mode défini dans la configuration iDRAC	État de la fonction d'identité d'E/S dans l'iDRAC	Configuration XML	Stratégie de persistance	Effacer la stratégie de persistance : adresses virtuelles
Flex Address activé	Mode FlexAddress	Activée	Gestion des adresses virtuelles (VAM) configurée	VAM configuré persiste	Défini sur Flex Address
Flex Address activé	Mode FlexAddress	Activée	VAM non configuré	Défini sur Flex Address	Pas de persistance - Défini sur Flex Address

Tableau 31. Comportement de Virtual/Flex Address et de la stratégie de persistance (suite)

État de la fonction FlexAddress dans le CMC	Mode défini dans la configuration iDRAC	État de la fonction d'identité d'E/S dans l'iDRAC	Configuration XML	Stratégie de persistance	Effacer la stratégie de persistance : adresses virtuelles
Flex Address activé	Mode Flex Address	Disabled (désactivé)	Configuré à l'aide du chemin défini dans le Lifecycle Controller	Définir sur Flex Address pour ce cycle	Pas de persistance - Défini sur Flex Address
Flex Address activé	Mode Flex Address	Disabled (désactivé)	VAM non configuré	Défini sur Flex Address	Défini sur Flex Address
Flex Address désactivé	Mode Flex Address	Activée	VAM configuré	VAM configuré persiste	Persistance uniquement : l'effacement n'est pas possible
Flex Address désactivé	Mode Flex Address	Activée	VAM non configuré	Définir sur l'adresse MAC du matériel	Pas de prise en charge de la persistance. Dépend du comportement de la carte
Flex Address désactivé	Mode Flex Address	Disabled (désactivé)	Configuré à l'aide du chemin défini dans le Lifecycle Controller	La configuration du Lifecycle Controller persiste pour ce cycle	Pas de prise en charge de la persistance. Dépend du comportement de la carte
Flex Address désactivé	Mode Flex Address	Disabled (désactivé)	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel
Flex Address activé	Mode console	Activée	VAM configuré	VAM configuré persiste	Tant la persistance que l'effacement doivent fonctionner
Flex Address activé	Mode console	Activée	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel
Flex Address activé	Mode console	Disabled (désactivé)	Configuré à l'aide du chemin défini dans le Lifecycle Controller	La configuration du Lifecycle Controller persiste pour ce cycle	Pas de prise en charge de la persistance. Dépend du comportement de la carte
Flex Address désactivé	Mode console	Activée	VAM configuré	VAM configuré persiste	Tant la persistance que l'effacement doivent fonctionner
Flex Address désactivé	Mode console	Activée	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel
Flex Address désactivé	Mode console	Disabled (désactivé)	Configuré à l'aide du chemin défini dans le Lifecycle Controller	La configuration du Lifecycle Controller persiste pour ce cycle	Pas de prise en charge de la persistance. Dépend du comportement de la carte
Flex Address activé	Mode console	Disabled (désactivé)	VAM non configuré	Définir sur l'adresse MAC du matériel	Définir sur l'adresse MAC du matériel

Comportement du système pour l'identité d'E/S et FlexAddress

Tableau 32. Comportement du système pour l'identité d'E/S et FlexAddress

	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(es)	Désactivé		FlexAddress depuis CMC	Spécification par FlexAddress
	Non Applicable (N/A), activé ou désactivé	Activé(es)	Oui : Nouveau ou persistant	Adresse virtuelle de l'agent distant	Spécification par FlexAddress
			Non	Adresse virtuelle effacée	
	Désactivé	Désactivé			
Serveur avec fonction de stratégie de persistance VAM	Activé(es)	Désactivé		FlexAddress depuis CMC	Spécification par FlexAddress
	Activé(es)	Activé(es)	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(es)	Oui : Nouveau ou persistant	Adresse virtuelle de l'agent distant	Paramètre de stratégie par l'agent à distance
			Non	Adresse virtuelle effacée	
	Désactivé	Désactivé			

Activation ou désactivation de l'optimisation d'identité d'E/S

Normalement, après le démarrage du système, les périphériques sont configurés, puis les périphériques sont initialisés après un redémarrage. Vous pouvez configurer la fonction Optimisation de l'identité d'E/S pour effectuer un démarrage optimal. Si la fonction est activée, elle définit les attributs d'adresse virtuelle, d'initiateur et de cible de stockage après la réinitialisation du périphérique et avant son initialisation, éliminant ainsi le besoin d'un deuxième redémarrage du BIOS. L'opération de configuration et de démarrage du périphérique survient lors du démarrage unique du système et est optimisée pour les performances du temps d'amorçage.

Avant d'activer l'optimisation de l'identité d'E/S, assurez-vous que :

- Vous détenez des privilèges de connexion, de configuration et de contrôle du système.
- Le BIOS, l'iDRAC et les cartes réseau sont mis à jour à la version la plus récente du micrologiciel. Pour plus d'informations sur les versions prises en charge, reportez-vous à Cartes prises en charge pour l'optimisation d'identité d'E/S , page 186 et à Supported nic firmware version for i/o identity optimization (Versions du micrologiciel des cartes réseau prises en charge pour l'optimisation de l'identité des E/S).

Après l'activation de la fonction d'optimisation d'identité d'E/S, exportez le fichier de configuration XML d'iDRAC, modifiez les attributs d'identité d'E/S requis dans le fichier de configuration XML et réimportez le fichier sur iDRAC.

Pour obtenir la liste des attributs d'optimisation d'identité d'E/S que vous pouvez modifier dans le fichier de configuration XML, voir le document *Profil de carte réseau* disponible sur **delltechcenter.com/idrac**.

REMARQUE : Ne modifiez pas les attributs autres que ceux d'optimisation d'identité d'E/S.

Activation ou désactivation de l'optimisation d'identité d'E/S via l'interface Web

Pour activer ou désactiver l'optimisation d'identité d'E/S :

1. Dans l'interface Web iDRAC, accédez à **Présentation générale** > **Matériel** > **Périphériques réseau**.
   La page **Périphériques réseau** s'affiche.
2. Cliquez sur l'onglet **I/O Identity Optimization (Optimisation d'identité d'E/S)** et sélectionnez l'option **I/O Identity Optimization (Optimisation d'identité d'E/S)** pour activer cette fonction. Pour la désactiver, désélectionnez 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
```

Configuration des paramètres de la stratégie de persistance

En vous servant de l'identité d'E/S, vous pouvez configurer des stratégies indiquant le comportement de redémarrage du système et de cycle d'alimentation qui détermine la persistance ou le déstockage 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 fonction **Persistence Policy (Stratégie de persistance)** risque de ne pas fonctionner correctement lorsqu'elle est définie sur la valeur par défaut, si l'attribut **VirtualAddressManagement** est défini sur le mode **FlexAddress** sur l'iDRAC et si la fonction FlexAddress est désactivée dans le CMC. Assurez-vous de définir l'attribut **VirtualAddressManagement** sur le mode **Console** dans l'iDRAC ou d'activer la fonction FlexAddress dans le CMC.

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 d'événements SNMP, de courrier électronique ou de WS. Les journaux sont également inclus dans le syslog distant.

Tableau 33. 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

Tableau 33. Valeurs par défaut de la stratégie de persistance (suite)

Stratégie de persistance	Perte d'alimentation CA	Démarrage à froid	Démarrage à chaud
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 permet pas de récupérer l'adresse virtuelle. Vous devez définir l'adresse virtuelle à nouveau après avoir activé la stratégie persistante.

REMARQUE : S'il y a une stratégie de persistance 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 la modification de VirtualizationMode ou de 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 pour définir explicitement des attributs d'adresse virtuelle sur des zéros et les valeurs de l'initiateur et des cibles de stockage comme défini dans Valeurs par défaut des cibles de stockage et de l'initiateur iSCSI , page 191.

Concepts associés

Activation ou désactivation de l'optimisation d'identité d'E/S , page 189

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 iDRAC, accédez à **Présentation générale** > **Matériel** > **Périphériques réseau**.
   La page **Périphériques réseau** s'affiche.
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 :
   - **Perte de l'alimentation CA** : les paramètres d'adresse virtuelle ou de cible sont conservés en cas de perte d'alimentation CA.
   - **Démarrage à froid** : les paramètres d'adresse virtuelle ou de cible sont conservés en cas de redémarrage à froid.
   - **Démarrage à chaud** : les paramètres d'adresse virtuelle ou de cible sont conservés en cas de redémarrage à chaud.
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**

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 34. 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	::
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	

Tableau 35. 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	
ConnectSecondTgt	Désactivé	Désactivé

Tableau 35. Valeurs par défaut des attributs de cibles de stockage iSCSI (suite)

Attributs de cibles de stockage iSCSI	Valeurs par défaut en mode IPv4	Valeurs par défaut en mode IPv6
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	

13

Gestion de périphériques de stockage

Depuis iDRAC version 2.00.00.00, iDRAC développe sa gestion sans agent pour inclure la configuration directe des nouveaux contrôleurs PERC9. Il vous permet de configurer à distance les composants de stockage connectés à votre système au moment de l'exécution. Ces composants comprennent des contrôleurs RAID et non RAID et les canaux, ports, boîtiers et disques qui leur sont associés.

La détection, la topologie, la surveillance de l'intégrité et la configuration complètes du sous-système de stockage sont réalisées dans la structure CEM (Comprehensive Embedded Management) en communiquant avec les contrôleurs PERC interne et externe via l'interface I2C selon le protocole MCTP. Pour une configuration en temps réel, CEM prend en charge les contrôleurs PERC9. La version du micrologiciel des contrôleurs PERC9 doit être 9.1 ou ultérieure.

Avec iDRAC, vous pouvez effectuer la plupart des fonctions disponibles dans OpenManage Storage Management, notamment les commandes de configuration (par exemple, création d'un disque virtuel) en temps réel (sans redémarrage). Vous pouvez configurer RAID avant d'installer le système d'exploitation.

Vous pouvez configurer et gérer les fonctions du contrôleur sans accéder au BIOS. Ces fonctions incluent la configuration des disques virtuels et l'application des niveaux de RAID et des disques de secours pour la protection des données. Vous pouvez également exécuter d'autres fonctions du contrôleur telles que la reconstruction et le dépannage. Vous pouvez protéger vos données en configurant la redondance des données ou en attribuant des disques de secours.

Les périphériques de stockage sont les suivants :

- Pour les contrôleurs : la plupart des systèmes d'exploitation (SE) ne lisent pas et n'écrivent pas de données directement à partir des disques, mais envoient plutôt des instructions de lecture et d'écriture à un contrôleur. Le contrôleur est le matériel de votre système qui interagit directement avec les disques pour écrire et récupérer des données. Un contrôleur dispose de connecteurs (canaux ou ports) qui sont raccordés à un ou plusieurs disques physiques ou à une enceinte contenant des disques physiques. Les contrôleurs RAID peuvent chevaucher les limites des disques pour créer une quantité accrue d'espace de stockage ou un disque virtuel, en utilisant la capacité de plusieurs disques. Les contrôleurs peuvent aussi effectuer d'autres tâches, comme lancer des recréations, initialiser des disques, et plus encore. Pour effectuer leurs tâches, les contrôleurs nécessitent des logiciels spécifiques appelés micrologiciel et pilotes. Pour fonctionner correctement, le contrôleur doit avoir la version minimale requise du micrologiciel et des pilotes installée. Les divers contrôleurs lisent et écrivent les données et exécutent les tâches différemment. Il vous sera utile de connaître ces fonctionnalités pour gérer votre stockage de la façon la plus efficace.
- Les disques ou périphériques physiques résident dans une enceinte ou sont connectés au contrôleur. Sur un contrôleur RAID, les disques ou périphériques physiques permettent de créer des disques virtuels.
- Disque virtuel : fait référence au stockage créé par un contrôleur RAID à partir d'un ou de plusieurs disques physiques. Même si un disque virtuel peut être créé à partir de plusieurs disques physiques, il est considéré par le système d'exploitation comme un disque unique. Selon le niveau de RAID utilisé, le disque virtuel conserve les données redondantes en cas de problème de disque ou peut disposer d'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.
- Fond de panier : similaire à une enceinte. Dans un fond de panier, le connecteur de contrôleur et les disques physiques sont reliés à l'enceinte, cependant il ne dispose pas des fonctionnalités de gestion (capteurs de température, alarmes, etc.) associées aux enceintes externes. Les disques physiques peuvent faire partie d'une enceinte ou être reliés au fond de panier d'un système.

En plus de la gestion des disques physiques contenus dans l'enceinte, vous pouvez surveiller l'état des ventilateurs, des blocs d'alimentation et des capteurs de température de l'enceinte. Les enceintes sont enfichables à chaud. L'enfichage à chaud représente l'ajout d'un composant sur un système alors que le système d'exploitation est en fonctionnement.

Le micrologiciel le plus récent doit être installé sur les périphériques physiques connectés au contrôleur. Pour la dernière version du micrologiciel prise en charge, contactez votre fournisseur de service.

Les événements de stockage de PERC sont adressés selon le cas vers des interruptions SNMP et des événements WSMAN. Toutes les modifications apportées aux configurations de stockage sont journalisées dans le journal Lifecycle.

Tableau 36. Capacité PERC

Capacité PERC	Contrôleur prenant en charge la configuration CEM (PERC 9.1 ou ultérieure)	Contrôleur non compatible avec la configuration CEM (PERC 9.0 et antérieure)
En temps réel	S'il n'existe aucune tâche en attente ou planifiée pour le contrôleur, la configuration est appliquée.	La configuration est appliquée. Un message d'erreur s'affiche. La création de la tâche échoue et vous ne pouvez pas créer de

Tableau 36. Capacité PERC (suite)

Capacité PERC	Contrôleur prenant en charge la configuration CEM (PERC 9.1 ou ultérieure)	Contrôleur non compatible avec la configuration CEM (PERC 9.0 et antérieure)
	Si des tâches sont en cours ou planifiées pour ce contrôleur, les tâches doivent être annulées. Sinon, vous devez attendre que les tâches se terminent avant d'appliquer la configuration au moment de l'exécution. Le temps d'exécution ou le temps réel signifie qu'aucun redémarrage n'est nécessaire.	tâches en temps réel à l'aide de l'interface Web.
Différées	Si toutes les opérations set sont différées, la configuration est préparée et appliquée après le redémarrage de l'ordinateur ou elle est appliquée en temps réel.	La configuration est appliquée après le redémarrage de l'ordinateur

Concepts associés

Présentation des concepts RAID , page 195
Inventaire et surveillance des périphériques de stockage , page 207
Affichage de la topologie des périphériques de stockage , page 208
Gestion des contrôleurs , page 217
Gestion des disques physiques , page 208
Gestion des boîtiers ou des fonds de panier , page 229
Gestion des SSD PCIe , page 225
Gestion de disques virtuels , page 211
Clignotement ou annulation du clignotement des LED des composants , page 236

Références connexes

Contrôleurs pris en charge , page 204
Boîtiers pris en charge , page 205
Récapitulatif des fonctions prises en charge pour les périphériques de stockage , page 205

Sujets :

- Présentation des concepts RAID
- Contrôleurs pris en charge
- Boîtiers pris en charge
- Récapitulatif des fonctions prises en charge pour les périphériques de stockage
- Inventaire et surveillance des périphériques de stockage
- Affichage de la topologie des périphériques de stockage
- Gestion des disques physiques
- Gestion de disques virtuels
- Gestion des contrôleurs
- Gestion des SSD PCIe
- Gestion des boîtiers ou des fonds de panier
- Choix du mode de fonctionnement pour l'application des paramètres
- Affichage et application des opérations en attente
- Périphériques de stockage : scénarios d'opérations d'application
- Clignotement ou annulation du clignotement des LED des composants

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.

RAID

RAID est une technologie permettant de gérer le stockage des données sur les disques physiques se trouvant sur votre système ou y étant reliés. L'aspect clé de la technologie RAID est sa capacité à répartir les données sur les disques physiques afin que la capacité de stockage combinée de plusieurs disques physiques puisse être considérée comme un seul espace disque étendu. Un autre aspect clé de la technologie RAID est sa capacité à conserver les données redondantes qui peuvent être utilisées pour restaurer les données en cas d'une panne de disque. RAID recourt à différentes techniques, telles que la segmentation, la mise en miroir et la parité, pour stocker et reconstruire les données. Il existe différents niveaux de RAID qui utilisent différentes méthodes pour le stockage et la reconstruction des données. Les niveaux de RAID possèdent différentes caractéristiques en matière de performances de lecture/écriture, de protection des données et de capacité de stockage. Certains 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 votre priorité : les performances, la protection ou la capacité de stockage.

REMARQUE : Le RAB (RAID Advisory Board) définit les spécifications servant à implémenter la technologie RAID. Bien que le RAB définisse les niveaux de RAID, l'implémentation commerciale des niveaux de RAID par différents fournisseurs peut dépendre des spécifications RAID. Une implémentation utilisée par un fournisseur particulier peut affecter les performances de lecture-écriture et le degré de redondance des données.

RAID matériel et logiciel

La technologie RAID peut être implémentée avec le matériel ou le logiciel. Un système qui utilise un RAID de matériel dispose d'un contrôleur RAID qui implémente les niveaux de RAID et traite les lectures-écritures sur les disques physiques. Lorsque le RAID de logiciel fournit par le système d'exploitation est utilisé, le système d'exploitation implémente les niveaux de RAID. Pour cette raison, utiliser le RAID de logiciel seul peut amoindrir les performances du système. Cependant, vous pouvez utiliser le RAID de logiciel en plus des volumes du RAID de matériel pour obtenir de meilleures performances et une meilleure variété dans la configuration des volumes RAID. Par exemple, vous pouvez mettre en miroir une paire de volumes de RAID 5 de matériel sur deux contrôleurs RAID pour fournir une redondance des contrôleurs RAID.

Concepts de RAID

La technologie RAID utilise des techniques particulières pour l'écriture des données sur les disques. Ces techniques permettent au RAID de fournir une redondance des données ou de meilleures performances. Ces techniques comprennent :

- Mise en miroir : duplication des données d'un disque physique à un autre. La mise en miroir fournit une redondance des données en conservant deux copies des mêmes données sur différents disques physiques. Si un des disques du miroir échoue, le système peut continuer de fonctionner à l'aide du disque qui fonctionne. Les deux côtés du miroir contiennent toujours les mêmes données. N'importe quel côté peut agir en tant que côté opérationnel. Un groupe de disques RAID mis en miroir est comparable (en matière de performances) à un groupe de disques RAID 5 dans le cadre des opérations de lecture, cependant il offre des opérations d'écriture plus rapides.
- Segmentation : le processus de segmentation des disques écrit les données sur tous les disques physiques d'un disque virtuel. Chaque bande est composée d'adresses de données de disques virtuels consécutives qui sont adressées dans des unités de taille fixe à chaque disque physique du disque virtuel de manière séquentielle. Par exemple, si le disque virtuel comprend cinq disques physiques, la segmentation écrit les données sur les disques physiques un à cinq sans répéter les écritures sur un même disque. L'espace consommé par une bande est le même sur chaque disque physique. La partie de la bande qui réside sur un disque physique est est un segment de bande. La segmentation même ne fournit aucune redondance de données. La segmentation combinée à la parité fournit une redondance des données.
- Taille de bande : l'espace disque total consommé par une bande qui ne comprend pas de disque de parité. Par exemple, une bande qui contient un espace de disque de 64 Ko et 16 Ko de données sur chaque disque de la bande a une taille de bande de 64 Ko et un segment de bande de 16 Ko.
- Segment de bande : un segment de bande est la partie d'une bande qui réside sur un seul disque physique.
- Taille du segment de bande : l'espace disque consommé par un segment de bande. Par exemple, une bande qui contient un espace de disque de 64 Ko et 16 Ko de données sur chaque disque de la bande a un segment de bande de 16 Ko et une bande de 64 Ko.
- Parité : la parité fait référence aux données redondantes conservées à l'aide d'un algorithme en combinaison avec la segmentation. Lorsque l'un des disques segmentés échoue, les données peuvent être reconstruites depuis les 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 de RAID

Chaque niveau de RAID se sert d'une certaine combinaison de mise en miroir, segmentation et parité pour fournir une redondance des données ou de meilleures performances de lecture et d'écriture. Pour des informations spécifiques sur chaque niveau de RAID, voir Sélection des niveaux de RAID.

Organisation du stockage des données à des fins de disponibilité et de performances

La technologie RAID fournit différentes méthodes ou niveaux de RAID pour l'organisation du stockage sur disque. Certains niveaux de RAID conservent les données redondantes de manière à ce que vous puissiez restaurer les données suite à une panne de disque. Différents niveaux de RAID signifie également des performances accrues ou amoindrie des E/S (lecture et écriture) d'un système.

Conserver des données redondantes nécessite l'utilisation de disques physiques supplémentaires. Plus vous utilisez de disques physiques, plus il est probable qu'une panne de disque survienne. Étant donné les différences qui existent entre les performances et la redondance des E/S, un niveau de RAID peut largement suffire, comparé à un autre selon les applications dans l'environnement de fonctionnement et 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 et tolérance aux pannes : cela fait référence à la capacité d'un système à maintenir ses opérations et fournir un accès aux données même lorsque l'un de ses composants est en panne. Dans les volumes RAID, la disponibilité ou la tolérance aux pannes s'obtient en maintenant les données redondantes. Les données redondantes incluent les miroirs (données en double) et les informations de parité (reconstruction des données à l'aide d'un algorithme).
- Performances : les performances de lecture-écriture peuvent être accrues ou amoindries selon le niveau de RAID que vous sélectionnez. Certains niveaux de RAID peuvent être plus appropriés que d'autres selon les applications.
- Économie : le maintient des données redondantes ou des informations de parité associées aux volumes RAID nécessite un espace disque supplémentaire. Lorsque les données sont temporairement facilement reproduites ou non essentielles, le coût accru de la redondance des données peut ne pas être justifiable.
- Intervalle moyen entre les défaillances (MTBF) : utiliser des disques supplémentaires pour conserver la redondance des données peut également rendre plus probable la survenue d'une panne de disque à tout moment. Bien qu'il soit impossible d'éviter une panne dans les cas où la redondance des données est requise, cela affecte négativement le personnel de support du système de votre organisation.
- Volume : un volume fait référence à un disque virtuel non RAID composé d'un seul disque. Vous pouvez créer des volumes à l'aide d'utilitaires externes tels que O-ROM <Ctrl> <r>. Storage Management (la gestion du stockage) ne prend pas en charge la création de volumes. Cependant, vous pouvez afficher les volumes et utiliser les disques de ces volumes pour la création de nouveaux disques virtuels ou pour étendre la capacité en ligne (OCE) des disques virtuels existants, à condition que de l'espace soit disponible.

Choix des niveaux de RAID

Vous pouvez utiliser RAID pour contrôler le stockage des données sur plusieurs disques. Chaque niveau de RAID ou concaténation a différentes caractéristiques de performances et de protection des données.

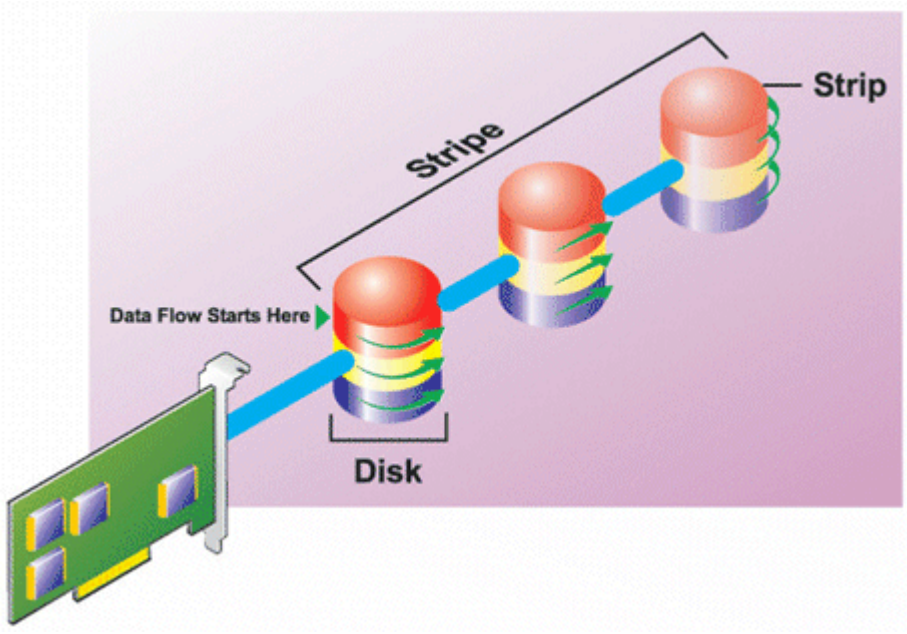
REMARQUE : Les contrôleurs PERC H3xx ne prennent pas en charge les niveaux RAID 6 et 60.

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 (segmentation)
- Niveau de RAID 1 (mise en miroir)
- Niveau de RAID 5 (segmentation avec parité distribuée)
- Niveau de RAID 6 (segmentation avec parité distribué supplémentaire)
- Niveau de RAID 50 (segmentation sur des ensembles de RAID 5)
- Niveau de RAID 60 (segmentation sur des ensembles de RAID 6)
- Niveau de RAID10 (segmentation sur des ensembles miroir)

Niveau de RAID 0 -segmentation

RAID 0 utilise la segmentation 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.

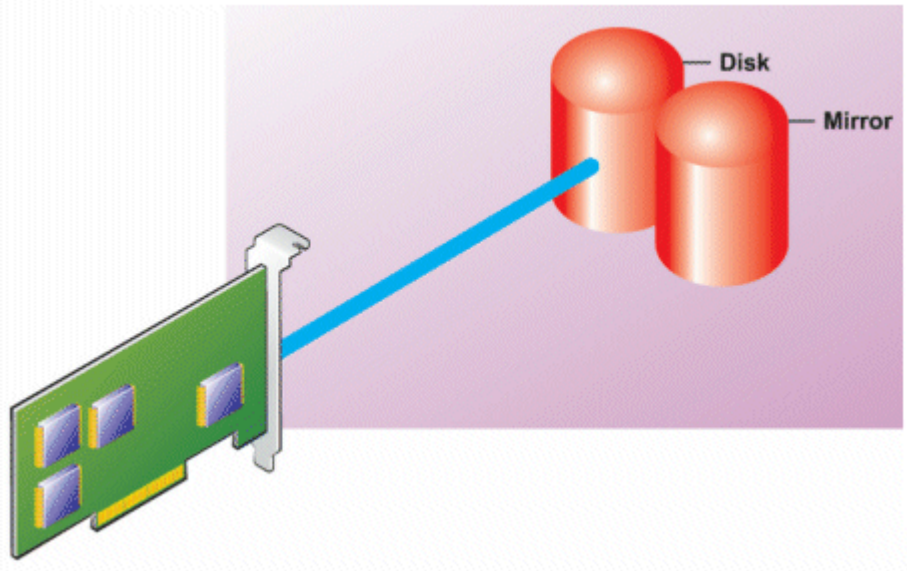


RAID 0

- 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 de redondance n'est conservée. Lorsqu'un disque échoue, le disque virtuel important échoue sans pouvoir recréer les données de quelque façon que ce soit.
- Les performances de lecture-écriture sont meilleures.

Niveau de RAID 1 - mise en miroir

RAID 1 constitue la méthode la plus simple de maintien des données redondantes. Avec RAID 1, les données sont mises en miroir ou dupliquées sur un ou plusieurs disques physiques. Si un disque physique échoue, vous pouvez reconstruire les données à partir de l'autre côté du miroir.



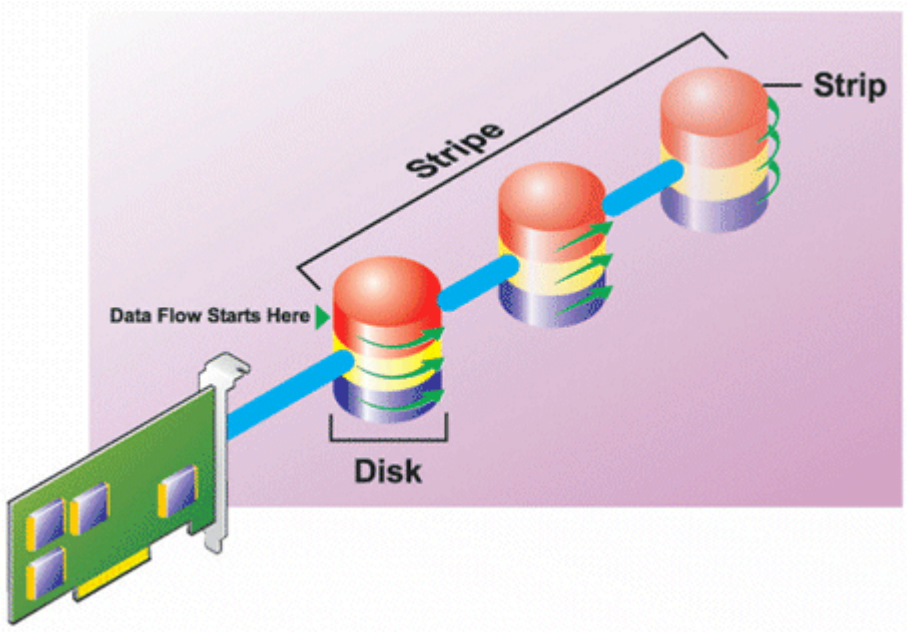
Caractéristiques de RAID 1 :

- Disques des groupes *n* + *n* comme disque virtuel unique d'une capacité de *n* disques. Les contrôleurs actuellement pris en charge par Storage Management permettent de sélectionner deux disques au moment de la création d'un RAID 1. Étant donné que ces disques sont en miroir, la capacité totale de stockage correspond à un disque.
- Les données sont répliquées sur les deux disques.
- Lorsqu'un disque échoue, le disque virtuel fonctionne encore. Les données sont lues depuis le 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 - segmentation avec parité distribuée

RAID 5 offre la redondance des données à l'aide de la répartition des données en combinaison avec les informations de parité. Plutôt que de dédier un disque physique à la parité, les informations de parités sont réparties sur tous les disques physiques du groupe de disques.

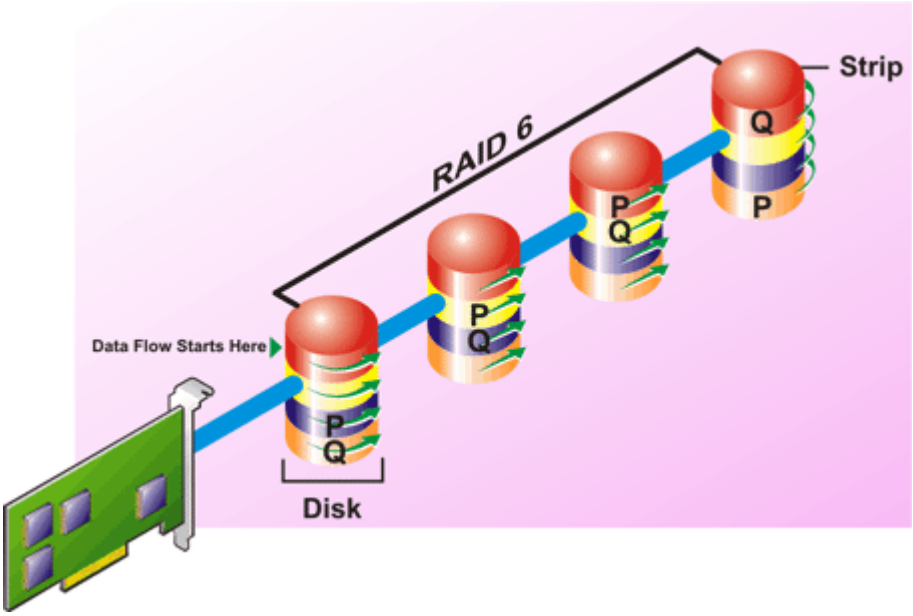


Caractéristiques de RAID 5 :

- 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.
- Si un disque échoue, le disque virtuel fonctionne encore, cependant il fonctionne en mode 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 - segmentation avec parité distribuée supplémentaire

RAID 6 offre la redondance des données à l'aide de la répartition des données en combinaison avec les informations de parité. Tout comme avec RAID 5, la parité est distribuée à l'intérieur de chaque bande. Toutefois, RAID 6 utilise un disque physique additionnel afin de conserver la parité, de telle façon que chaque bande dans le groupe de disques conserve deux blocs de données disposant des informations de parité. La parité additionnelle offre la protection des données dans le cas de deux pannes de disque. À l'image suivante, les deux ensembles d'informations de parité sont identifiés en tant que **P** et **Q**.



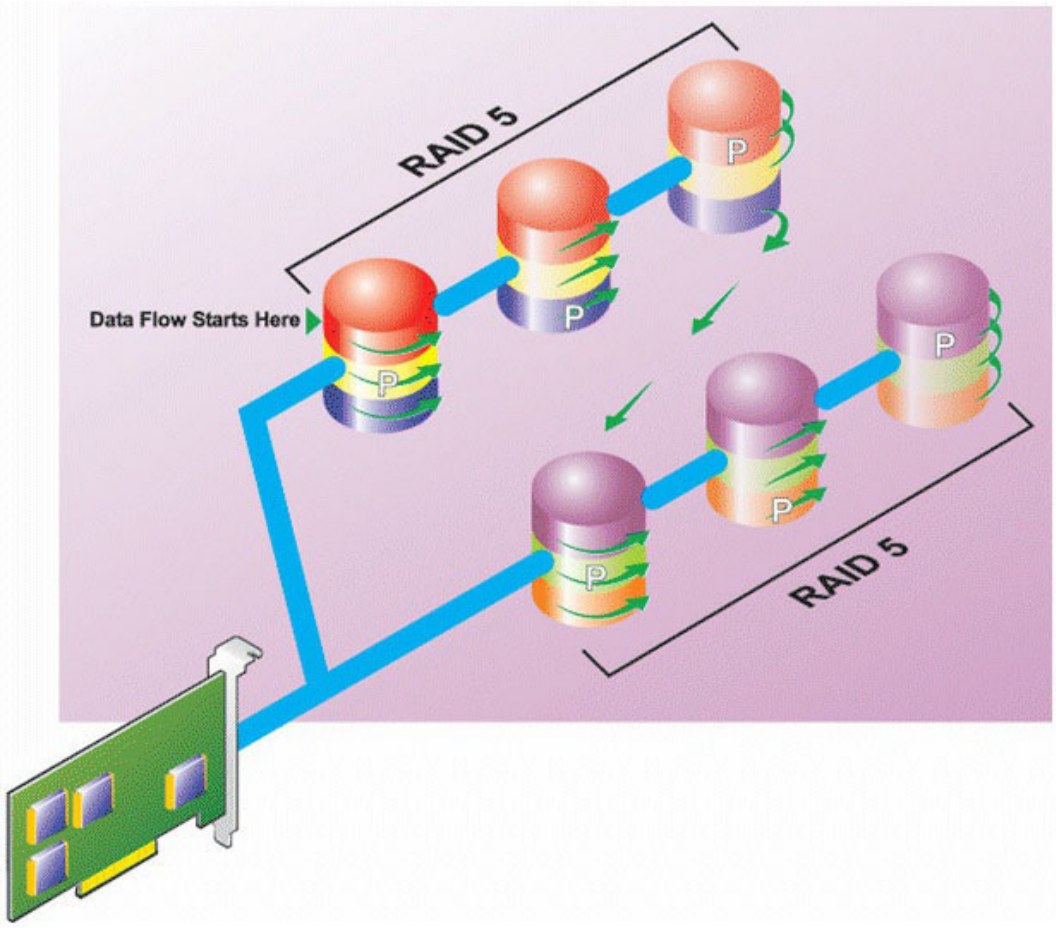
Caractéristiques de RAID 6 :

- 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 demeure fonctionnel avec jusqu'à deux pannes de disque. 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 cher en matière d'espace disque.

Niveau de RAID 50 - segmentation sur des ensembles de RAID 5

RAID 50 est segmenté sur plus d'une répartition de disques physiques. Par exemple, un groupe de disques RAID 5 qui est implémenté avec trois disques physiques et continue de fonctionner avec un groupe de disques composé de plus de trois disques physiques serait 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 ces derniers en disques dynamiques. Vous pouvez ensuite créer un volume dynamique qui est réparti sur tous les disques virtuels RAID 5.

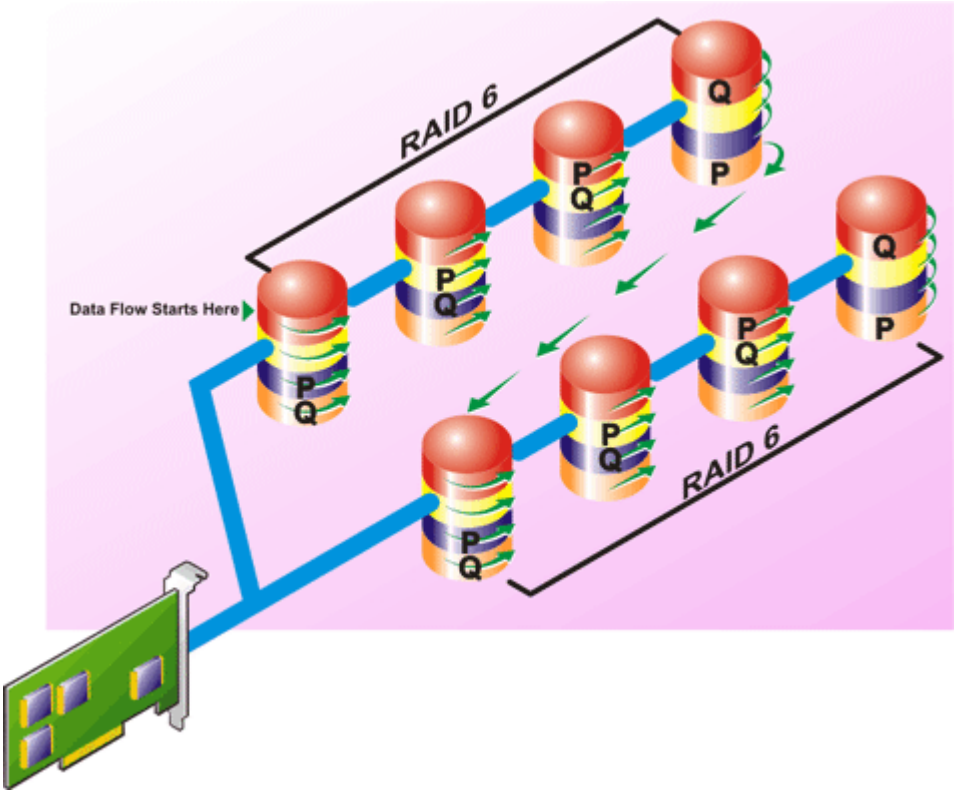


Caractéristiques de RAID 50 :

- Disques de groupes *n***s* comme disque virtuel important 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 segmentées sur toutes les répartitions. RAID 50 est plus cher en matière d'espace disque.

Niveau de RAID 60 - segmentation sur des ensembles de RAID 6

RAID 60 est segmentée sur plus d'une répartition de disques physiques configurés en tant que RAID 6. Par exemple, un groupe de disques RAID 6 qui est implémenté avec quatre disques physiques et qui continue de fonctionner avec un groupe de disques composé de quatre disques physiques ou plus serait un RAID 60.

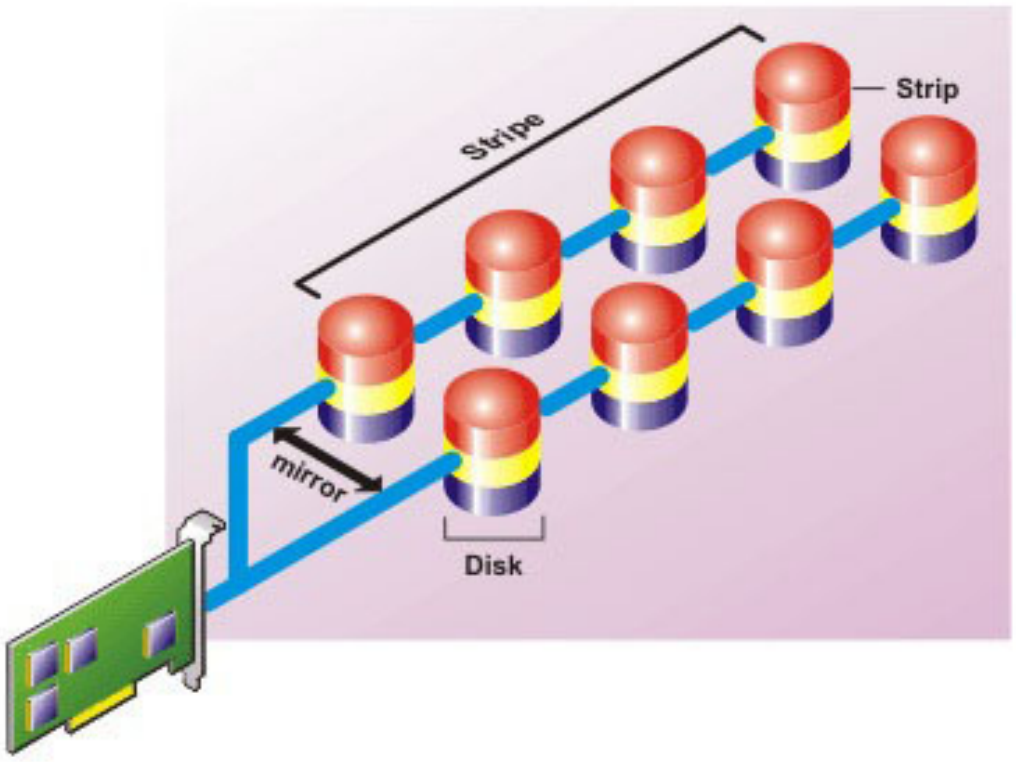


Caractéristiques de RAID 60 :

- Regroupe les disques *n***s* comme disque virtuel important 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 cher en matière d'espace disque.

Niveau de RAID 10 -segmentation-miroirs

Le RAB considère que le niveau de RAID 10 est une implémentation d'un niveau de RAID 1. RAID 10 combine les disques physiques mis en miroir (RAID 1) avec la segmentation des données (RAID 0). Avec RAID 10, les données sont segmentées sur plusieurs disques physiques. Le groupe de disques segmentés est alors mis en miroir sur un autre ensemble de disques physiques. RAID 10 peut être considéré comme un *miroir de bandes*.



Caractéristiques de RAID 10 :

- Disques de groupes *n* comme disque virtuel important avec une capacité de (*n*/2) disques, où *n* est un nombre entier pair.
- Les images miroirs des données sont segmentées sur les ensembles de disques physiques. Ce niveau fournit la redondance via la mise en miroir.
- Lorsqu'un disque échoue, le disque virtuel fonctionne encore. 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 les plus courants. 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 37. Comparaison des performances des niveaux RAID

Adresse RAID	Disponibilité 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	NA	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 critiques
RAID 5	Bon	Lectures séquentielles : bon. Lecture transactionnelles : Très bon	Bien, sauf si vous utilisez le cache d'écriture différée	Bien	N + 1 (N = au moins deux disques)	Pour les bases de données et d'autres usages transactionnels

Tableau 37. Comparaison des performances des niveaux RAID (suite)

Adresse RAID	Disponibilité 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	Bien	Bon	2N x X	Environnements intensifs de données (enregistrements importants)
RAID 50	Bon	Très bon	Bien	Bien	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 critiques. Pour les bases de données et d'autres usages transactionnels intensifs de lecture
RAID 60	Excellent	Très bon	Bien	Médiocre	X x (N + 2) (N = au moins 2)	Informations critiques. Environnements transactionnels de taille moyenne ou usages de données intensifs
N = Nombre de disques physiques X = Nombre d'ensembles de RAID						

Contrôleurs pris en charge

Contrôleurs RAID pris en charge

Les interfaces iDRAC prennent en charge les contrôleurs PERC9 suivants :

- PERC H830
- PERC H730P
- PERC H730
- PERC H330

Les interfaces iDRAC prennent en charge les contrôleurs PERC8 suivants :

- PERC H810
- PERC H710P
- PERC H710
- PERC H310

Les interfaces iDRAC prennent en charge les contrôleurs PERC modulaires suivants :

- PERC FD33xS
- PERC FD33xD

REMARQUE : Pour plus d'informations sur la configuration et la modification du mode de contrôleur sur les contrôleurs PERC FD33xS et PERC FD33xD, voir le *Dell Chassis Management Controller Version 1.2 for PowerEdge FX2/FX2s User's Guide*

(Guide d'utilisation du Dell Chassis Management Controller Version 1.2 pour PowerEdge FX2/FX2s) disponible à l'adresse **dell.com/support/manuals**.

Contrôleurs non RAID pris en charge

L'interface iDRAC prend en charge le contrôleur externe HBA SAS 12 Gbit/s, le contrôleur interne HBA330, et les lecteurs SATA uniquement pour le contrôleur interne HBA330.

Boîtiers pris en charge

L'iDRAC prend en charge les boîtiers MD1200, MD1220, MD1400 et MD1420.

REMARQUE : Les RBOD (Redundant Array of Inexpensive Disks) qui sont connectés aux contrôleurs HBA ne sont pas pris en charge.

Récapitulatif des fonctions prises en charge pour les périphériques de stockage

Le tableau suivant fournit les fonctions prises en charge par les périphériques de stockage par le biais d'iDRAC.

REMARQUE : Les fonctionnalités telles que la préparation au retrait et l'activation ou la désactivation du clignotement LED de composant ne s'appliquent pas aux cartes SSD PCIe HHHL.

Tableau 38. Fonctions prises en charge pour les périphériques de stockage

Nom de la fonction	Contrôleurs PERC 9						Contrôleurs PERC 8				SSD PCIe
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Affecter ou annuler l'affectation d'un disque physique comme disque de secours global	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Créez des disques virtuels	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Modifiez les règles de cache des disques virtuels	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Vérifiez la cohérence de disque virtuel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Annuler la vérification de cohérence	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet
Initialisez des disques virtuels	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Annuler l'initialisation	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet

Tableau 38. Fonctions prises en charge pour les périphériques de stockage (suite)

Nom de la fonction	Contrôleurs PERC 9						Contrôleurs PERC 8				SSD PCIe
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Crypter des disques virtuels	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Affectez ou annulez l'affectation d'un disque de secours dédié	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Supprimer des disques virtuels	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Définir le mode de lecture cohérente	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Zones non configurées de la lecture cohérente	En temps réel (uniquement à partir de l'interface Web)	En temps réel (uniquement à partir de l'interface Web)	En temps réel (uniquement à partir de l'interface Web)	En temps réel (uniquement à partir de l'interface Web)	En temps réel (uniquement à partir de l'interface Web)	En temps réel (uniquement à partir de l'interface Web)	Intermédiaire (uniquement à partir de l'interface Web)	Intermédiaire (uniquement à partir de l'interface Web)	Intermédiaire (uniquement à partir de l'interface Web)	Intermédiaire (uniquement à partir de l'interface Web)	Sans objet
Mode de vérification de la cohérence	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Mode de recopie	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Mode d'équilibrage de charge	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Taux de vérification de la cohérence	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Taux de recréation	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Taux d'initialisation en arrière-plan	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Taux de reconstruction	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Importer une configuration étrangère	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet

Tableau 38. Fonctions prises en charge pour les périphériques de stockage (suite)

Nom de la fonction	Contrôleurs PERC 9						Contrôleurs PERC 8				SSD PCIe
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Importer automatiquement une configuration étrangère	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Effacez une configuration étrangère	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Réinitialiser la configuration d'un contrôleur	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Créez ou modifiez les clés de sécurité	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Différées	Différées	Différées	Différées	Sans objet
Faire l'inventaire et surveiller à distance l'intégrité des périphériques SSD PCIe	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	En temps réel
Préparez le retrait du SSD PCIe	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	En temps réel
Effacer les données en toute sécurité	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet	Différées
Configurer le mode du fond de panier	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet
Faites clignoter ou annulez le clignotement des LED des composants	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel	En temps réel
Basculez le mode du contrôleur	Différées	Différées	Différées	Différées	Différées	Différées	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet

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 et extenseurs PCIe
- Boîtiers contenant des modules EMM (Enclosure Management Modules), une alimentation électrique, un capteur de ventilateur et un capteur de température ;
- Disques physiques
- disques virtuels
- Batteries

Toutefois, RACADM et WSMAN affichent des informations pour la plupart des périphériques de stockage du système.

Les derniers événements de stockage et la topologie des périphériques de stockage sont également affichés.

Des alertes et des interruptions SNMP sont générées pour les événements de stockage. Les événements sont consignés dans le journal Lifecycle.

REMARQUE : Si vous énumérez sur un système la commande WSMAN de la vue de boîtier tandis qu'un câble du bloc d'alimentation est retiré, le statut principal de la vue du boîtier est signalée comme étant **en bon état opérationnel** au lieu d'être à l'état **avertissement**.

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 **Présentation générale** > **Stockage** > **Résumé** pour afficher le résumé des composants de stockage et les derniers événements consignés. Cette page est actualisée automatiquement toutes les 30 secondes.
- Accédez à **Présentation générale** > **Stockage** > **Topologie** pour afficher la vue de relation physique hiérarchique des principaux composants de stockage.
- Accédez à **Présentation** > **Stockage** > **Disques physiques** > **Propriétés** pour afficher les informations des disques physiques. La page **Propriétés des disques physiques** s'affiche.
- Accédez à **Présentation** > **Stockage** > **Disques virtuels** > **Propriétés** pour afficher les informations des disques virtuels. La page **Propriétés des disques virtuels** s'affiche.
- Accédez à **Présentation** > **Stockage** > **Contrôleurs** > **Propriétés** pour afficher les informations des contrôleurs RAID. La page **Propriétés des contrôleurs** s'affiche.
- Accédez à **Présentation** > **Stockage** > **Boîtiers** > **Propriétés** pour afficher les informations des boîtiers RAID. La page **Propriétés des boîtiers** s'affiche.

Vous pouvez également utiliser des filtres pour afficher les informations relatives à des périphériques spécifiques.

Pour plus d'informations sur les propriétés affichées et l'utilisation des options, voir l'*Aide en ligne d'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 en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Surveillance d'un fond de panier à l'aide de l'utilitaire de paramètres d'iDRAC

Dans l'utilitaire de Configuration d'iDRAC, accédez à **Récapitulatif du système**. La page **Configuration iDRAC.Récapitulatif du système** s'affiche. La section **Inventaire du fond de panier** affiche les informations sur le fond de panier. Pour en savoir plus 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 **Présentation** > **Stockage** > **Topologie**. La page **Topologie** affiche une représentation hiérarchique des composants de stockage dans le système.

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.

Concepts associés

Inventaire et surveillance des périphériques de stockage , page 207
Affectation ou annulation de l'affectation d'un disque physique comme disque de secours global , page 209

Affectation ou annulation de l'affectation d'un disque physique comme disque de secours global

Un disque de secours global est un disque de sauvegarde non utilisé faisant partie du groupe de disques. Les disques de secours restent en mode veille. Lorsqu'un disque physique utilisé dans un disque virtuel tombe en panne, le disque de secours attribué est activé pour remplacer le disque physique en panne sans que le système ne soit interrompu ou que votre intervention ne soit requise. Lorsqu'un disque de secours est activé, il recrée les données de tous les disques virtuels redondants qui utilisaient le disque physique problématique.

REMARQUE : À partir d'iDRAC v2.30.30.30 ou version ultérieure, vous pouvez ajouter des disques de secours globaux lorsque des disques virtuels ne sont pas créés.

Vous pouvez changer l'attribution de disque de secours en annulant l'attribution d'un disque et en en choisissant un autre, le cas échéant. Vous pouvez également attribuer plusieurs disques physiques en tant que disques de secours globaux.

L'attribution et l'annulation de l'attribution de disques de secours globaux doivent s'effectuer manuellement. Ces disques ne sont pas attribués à des disques virtuels spécifiques. Si vous souhaitez attribuer un disque de secours à un disque virtuel (il remplace tout disque physique en panne dans le disque virtuel), suivez Affectation ou annulation de l'affectation de disques de secours dédiés.

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.

Si vous réinitialisez la configuration, les disques virtuels sont supprimés et l'affectation de tous les disques de secours est annulée.

Vous devez être parfaitement informé des exigences relatives à la taille requise et des autres éléments à prendre en compte pour les disques de secours.

Avant d'affecter un disque physique comme disque de secours global :

- Assurez-vous que le Lifecycle Controller est activé.
- Si aucun disque n'est à l'état Prêt, insérez d'autres disques et assurez-vous que les disques sont à l'état Prêt.
- Si aucun disque virtuel n'est présent, créez au moins un disque virtuel.
- Si les disques physiques sont en mode non RAID, convertissez-les en mode RAID avec les interfaces iDRAC, notamment l'interface web iDRAC, RACADM ou WSMAN, ou avec <CTRL+R>.

Si vous avez affecté un disque physique en tant que disque de secours global en mode Ajouter à l'opération en attente, l'opération en attente est créée mais la tâche n'est pas créée. Si vous tentez ensuite d'annuler l'affectation de ce même disque en tant que disque de secours global, l'opération en attente d'attribution de disque de secours global est désactivée.

Si vous avez annulé l'affectation d'un disque physique en tant que disque de secours global en mode Ajouter à l'opération en attente, l'opération en attente est créée mais la tâche n'est pas créée. Si vous tentez ensuite d'affecter ce même disque en tant que disque de secours global, l'opération en attente d'annulation d'attribution de disque de secours global est désactivée.

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 iDRAC, accédez à **Présentation** > **Stockage** > **Disques physiques**.
   La page **Sélectionner des disques physiques** s'affiche.
2. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur pour afficher les disques physiques associés.
3. Pour affecter un disque en tant que disque de secours global, dans les menus déroulants dans la colonne **Action : affecter à tous**, sélectionnez **Disque de rechange global** pour un ou plusieurs disques physiques.
4. Pour annuler l'affectation d'un disque de secours global, dans les menus déroulants dans la colonne **Action : affecter à tous**, sélectionnez **Annuler l'affectation d'un disque de rechange** pour un ou plusieurs disques physiques.
5. Depuis le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez appliquer les paramètres.

6. Cliquez sur **Appliquer**.
   Les paramètres sont appliqués en fonction du mode de fonctionnement sélectionné.

Tâches associées

Choix du mode de fonctionnement à l'aide de l'interface Web , page 233

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 en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Tâches associées

Choix du mode de fonctionnement à l'aide de RACADM , page 234

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 iDRAC telles que l'interface web, RACADM ou WSMAN.
- en appuyant sur la combinaison de touches Ctrl+R lors du redémarrage du serveur, puis en sélectionnant le contrôleur requis.

REMARQUE : La conversion du mode n'est pas prise en charge sur les contrôleurs matériels PERC fonctionnant en mode HBA .

REMARQUE : La conversion au mode non RAID des contrôleurs PERC 8 est prise en charge uniquement pour les contrôleurs PERC H310 et H330.

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 WSMAN, 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 iDRAC, accédez à **Présentation** > **Stockage** > **Disques physiques** > **Configuration**.
   La fenêtre **Configuration** s'affiche.
2. Dans le menu déroulant **Contrôleur** , sélectionnez un contrôleur.
   Tous les disques physiques associés au contrôleur RAID s'affichent.
3. À partir de la zone de liste déroulante **Action - Affecter à tout**, sélectionnez l'option requise (**Convertir à RAID** ou **Convertir à non RAID**) pour tous les disques, ou sélectionnez l'option pour des disques dans le menu déroulant **Action** .
4. Depuis le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez appliquer les paramètres.
5. Cliquez sur **Appliquer**.
   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`.

Pour en savoir plus, voir l'*iDRAC RACADM Command Line Reference Guide (Guide de référence de la ligne de commande RACADM iDRAC)* disponible à l'adresse **dell.com/idracmanuals**.

Gestion de disques virtuels

Vous pouvez effectuer les opérations suivantes pour les disques virtuels :
- Créer
- Supprimer
- Modifier les règles
- Initialiser
- Vérifier la cohérence
- Annuler la vérification de cohérence
- Crypter des disques virtuels
- Affecter ou annuler l'affectation de disques de secours dédiés
- Faire clignoter la LED et Arrêter le clignotement de la LED de disques virtuels

REMARQUE : Vous pouvez gérer et surveiller 192 disques virtuels si la configuration automatique est activée via le BIOS du contrôleur PERC, l'infrastructure HII (Human Interface Infrastructure) et Dell OpenManage Server Administrator (OMSA).

Concepts associés

Création de disques virtuels , page 211
Modification des règles de cache des disques virtuels , page 213
Suppression de disques virtuels , page 213
Vérification de cohérence de disque virtuel , page 214
Initialisation des disques virtuels , page 214
Chiffrement de disques virtuels , page 215
Affectation ou annulation de l'affectation de disques de secours dédiés , page 215
Gestion de disques virtuels à l'aide de l'interface web , page 215
Gestion de disques virtuels à l'aide de RACADM , page 216

Création de disques virtuels

Pour mettre en œuvre des fonctions 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.
- Vous avez atteint la limite maximale de disques virtuels du groupe. 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 n'est pas en mode RAID. Dans ce cas, vous devez effectuer la conversion vers le mode RAID avec les interfaces iDRAC, notamment l'interface web iDRAC, RACADM, WSMAN 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.

Éléments à prendre en compte avant la création de disques virtuels

Avant la création des disques virtuels, tenez compte des éléments suivants :

- Noms de disques virtuels non stockés sur le contrôleur : les noms des disques virtuels que vous avez créés ne sont pas stockés sur le contrôleur. Cela signifie que si vous redémarrez avec un système d'exploitation différent, le nouveau système d'exploitation renommera peut-être le disque virtuel en utilisant ses propres conventions d'attribution 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 du groupe de disques. La version actuelle prend en charge le blocage de groupes de disques mixtes lors de la création de périphériques logiques.
- Les disques physiques étant liés aux groupes de disques, aucune combinaison de niveaux de RAID ne peut donc se produire sur un groupe de disques.
- Un nombre limité de disques physiques peuvent faire partie d'un disque virtuel. Ces limitations dépendent du contrôleur. Lorsque vous créez un disque virtuel, les contrôleurs prennent en charge un certain nombre de bandes et de répartitions (les méthodes de combinaison du stockage sur les disques physiques). Comme le nombre total de bandes et de répartitions est limité, le nombre de disques physiques pouvant être utilisés est aussi limité. Les limitations en matière 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 2. Ceci affecte les RAID 1 et RAID 10.
- Impossible de créer des disques virtuels sur les SSD PCIe.

Création de disques virtuels à l'aide de l'interface Web

Pour créer un disque virtuel :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Stockage** > **Disques virtuels** > **Créer**.
   La fenêtre **Créer un disque virtuel** s'affiche.
2. Dans la section **Paramètres**, effectuez l'une des opérations suivantes :
   a. Entrez le nom du disque virtuel.
   b. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur dont vous souhaitez créer le disque virtuel.
   c. 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.
   d. Sélectionnez le **Type de média**, **Taille de bande**, **Règle de lecture**, **Règles d'écriture** et **Règle de cache du disque**, **Capacité PI T10**.

      Seules les valeurs prises en charge par le contrôleur s'affichent dans les menus déroulants de ces propriétés.
   e. 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.
   f. Le champ **Nombre de répartitions** affiché est basé sur les disques physiques sélectionnés (étape 3). Vous ne pouvez pas définir cette valeur. Cette valeur est automatiquement calculée après la sélection de disques pour le niveau multi-RAID. Si vous avez sélectionné RAID 10 et si le contrôleur prend en charge un nombre impair de RAID 10, la valeur du nombre de répartitions ne s'affiche pas. Le contrôleur définit automatiquement la valeur appropriée.
3. Dans la section **Sélectionner les disques virtuels**, sélectionnez le nombre de disques physiques.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
4. Depuis le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez appliquer les paramètres.
5. Cliquez sur **Create Virtual Disk (Créer un disque virtuel)**.

   Les paramètres sont appliqués en fonction du **mode de fonctionnement** sélectionné.

Création de disques virtuels à l'aide de RACADM

Utilisez la commande `racadm storage createvd`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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 S130.

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.

REMARQUE : Les contrôleurs PERC d'anciennes générations prennent en charge les paramètres de règle de lecture **Pas de lecture anticipée**, **Lecture anticipée**, et **Lecture anticipée adaptative**. Avec les contrôleurs PERC 8 et PERC 9, les paramètres **Lecture anticipée** et **Lecture anticipée adaptative** offrent des fonctionnalités équivalentes au niveau du contrôleur. À des fins de rétrocompatibilité, certaines interfaces de gestion de systèmes et certains contrôleurs PERC 8 et PERC 9 permettent toujours de sélectionner la règle de lecture **Lecture anticipée adaptative**. S'il est possible de choisir entre les options **Lecture anticipée** et **Lecture anticipée adaptative** sur les contrôleurs PERC 8 et PERC 9, il n'y a aucune différence fonctionnelle.

- **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 d'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 panne 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 se trouvant sur le disque virtuel et supprime le disque virtuel de la configuration du contrôleur. Lors de la suppression de disques virtuels, tous les disques de secours globaux affectés peuvent être automatiquement désaffectés 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 affectés deviennent automatiquement des disques de secours globaux.

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 d'amorçage à partir de la bande latérale et indépendamment du système d'exploitation. Par conséquent, un message d'avertissement s'affiche avant de supprimer le disque virtuel.

Si vous supprimez un disque virtuel et que vous créez immédiatement un nouveau 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 jamais été supprimé. Dans ce cas, si vous ne souhaitez pas conserver les anciennes données après avoir recréé un nouveau disque virtuel, réinitialisez le disque virtuel.

Vérification de cohérence de disque virtuel

Cette opération vérifie l'exactitude des informations redondantes (parité). Cette tâche s'applique uniquement aux disques virtuels redondants. Lorsque cela s'avère nécessaire, la tâche de vérification de cohérence reconstruit les données redondantes. Si le disque virtuel est à l'état Dégradé, l'exécution d'une vérification de cohérence peut le remettre à l'état Prêt. Vous pouvez également effectuer une vérification de cohérence à l'aide de l'interface web ou de RACADM.

Vous pouvez également annuler l'opération de vérification de 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.

Initialisation des disques virtuels

L'initialisation des disques virtuels efface toutes les données sur le disque, mais ne modifie pas la configuration du disque virtuel. Vous devez initialiser un disque virtuel qui est configuré avant de pouvoir 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 uniquement à l'aide de l'interface Web iDRAC et non de RACADM.

Initialisation rapide

Utilisez la tâche Initialisation rapide pour initialiser tous les disques physiques inclus dans le disque virtuel. Elle met à jour les métadonnées sur les disques physiques de manière à ce que tout l'espace disque soit disponible pour les futures opérations d'écriture. L'initialisation peut être terminée rapidement, car les informations existantes sur les disques physiques ne sont pas effacées, mais les opérations d'écriture futures écrasent les informations qui restent sur les disques physiques.

L'initialisation rapide supprime uniquement le secteur d'amorçage et les informations de bande. Effectuez une initialisation rapide uniquement si vous avez peu de temps ou si les disques durs sont nouveaux ou inutilisés. L'initialisation rapide prend moins longtemps (généralement de 30 à 60 secondes).

PRÉCAUTION : L'exécution d'une initialisation rapide rend les données existantes inaccessibles.

La tâche Initialisation rapide n'écrit pas de zéros sur les blocs de disques des disques physiques. Comme la tâche Initialisation rapide n'effectue pas d'opérations d'écriture, elle dégrade moins le disque que la tâche Initialisation lente.

Une initialisation rapide sur un disque virtuel écrase les premiers et les derniers 8 Mo du disque virtuel, effaçant ainsi les enregistrements d'amorçage 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'initialisation complète (également appelée initialisation lente) initialise tous les disques physiques inclus dans le disque virtuel. Elle met à jour les métadonnées des disques physiques et efface toutes les données et tous les systèmes de fichiers existants. Vous pouvez effectuer l'initialisation complète une fois le disque virtuel créé. Il est préférable d'effectuer l'initialisation complète plutôt que l'initialisation

rapide si vous avez des problèmes avec un disque physique ou si vous soupçonnez qu'il contient des blocs de disque endommagés. L'opération d'initialisation complète réadresse les blocs endommagés et écrit des zéros sur tous les blocs de disques.

Si l'initialisation complète d'un disque virtuel est effectuée, l'initialisation en arrière-plan n'est pas obligatoire. 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 un processus d'initialisation en arrière-plan démarre sur le disque virtuel.

Il est recommandé de toujours faire une initialisation complète sur les disques qui contenaient des données auparavant. Une initialisation complète peut prendre 1 à 2 minutes par Go. La vitesse de l'initialisation dépend du modèle de contrôleur, de la vitesse des disques durs et de la version du micrologiciel.

L'initialisation complète initialise un disque physique à la fois.

REMARQUE : L'initialisation complète est prise en charge uniquement en temps réel. Seuls certains contrôleurs prennent en charge l'initialisation complète.

Chiffrement de disques virtuels

Lorsque le chiffrement est désactivé sur un contrôleur (c'est-à-dire, que la clé de sécurité est supprimée), il vous faudra activer le cryptage manuellement pour les disques virtuels créés à l'aide des disques SED. Si le disque virtuel est créé après l'activation du chiffrement sur le contrôleur, le disque virtuel est automatiquement chiffré. Il est automatiquement configuré en tant que disque virtuel chiffré, à moins que l'option de chiffrement activé ne soit désactivée pendant la création du disque virtuel.

Vous devez disposer du privilège de connexion et de contrôle du serveur pour gérer les clés de chiffrement.

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.

Seuls les disques physiques T10 PI (DIF) peuvent être affectés en tant que disques de secours aux disques virtuels T10 PI (DIF). Tous les disques non T10 PI (DIF) affectés en tant que disques de secours dédiés ne seront pas des disques de secours si T10 PI (DIF) est activé sur un disque virtuel ultérieurement.

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 aucune tâche n'est créée. Si vous tentez ensuite d'annuler l'affectation de ce même disque, 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 aucune tâche n'est créée. 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 : Pendant que l'opération d'exportation du journal est en cours, vous ne pouvez pas afficher les 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.

Gestion de disques virtuels à l'aide de l'interface web

1. Dans l'interface web d'iDRAC, accédez à **Présentation** > **Stockage** > **Disques virtuels** > **Gérer**.
   La page **Gestion de disques virtuels** s'affiche.
2. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur dont vous souhaitez gérer les disques virtuels.
3. Pour un ou plusieurs disques virtuels, à partir de chaque menu déroulant **Action**, sélectionnez une action.

   Vous pouvez spécifier plusieurs actions pour un lecteur virtuel. Lorsque vous sélectionnez une action, un menu déroulant **Action** supplémentaire s'affiche. Sélectionnez une autre action à partir de ce menu déroulant. Les actions sélectionnées n'apparaissent pas dans les menus déroulants **Action** supplémentaires. En outre, le lien **Supprimer** s'affiche en regard de l'action sélectionnée. Cliquez sur ce lien pour supprimer l'action sélectionnée.
   - **Supprimer**

- **Modifier la règle : cache de lecture** : vous pouvez définir la règle du cache de lecture sur l'une des options suivantes :
  - **No Read Ahead (Pas de lecture anticipée)**
  - **Read Ahead (Lecture anticipée)**
  - **Lecture anticipée adaptative**

    REMARQUE : Les précédentes générations de contrôleurs PERC prennent en charge les paramètres de règle de lecture **Pas de lecture anticipée**, **Lecture anticipée** et **Lecture anticipée adaptative**. Dans le cas de PERC 8 et PERC 9, les paramètres de **Lecture anticipée** et de **Lecture anticipée adaptative** offrent des fonctionnalités équivalentes au niveau du contrôleur. À des fins de compatibilité descendante, certaines interfaces de gestion de systèmes ainsi que les contrôleurs PERC 8 et 9 permettent encore de définir la règle de lecture sur **Lecture anticipée adaptative**. Bien qu'il soit possible de définir la **Lecture anticipée** ou **Lecture anticipée adaptative** sur PERC 8 ou PERC 9, il n'existe aucune différence fonctionnelle.
- **Modifier la règle : cache d'écriture** : vous pouvez définir la règle du cache d'écriture sur l'une des options suivantes :
  - **Écriture immédiate**
  - **Écriture différée**
  - **Forcer l'écriture différée**
- **Modifier la règle : cache de disque** : vous pouvez définir la règle du cache de disque sur l'une des options suivantes :
  - **Par défaut**
  - **Activée**
  - **Disabled (désactivé)**
- **Initialisation : rapide** : met à jour les métadonnées sur les disques physiques de manière à ce que tout l'espace disque soit disponible pour les opérations d'écriture futures. L'initialisation peut être terminée rapidement car les informations existantes sur les disques physiques ne sont pas effacées, mais les opérations d'écriture futures écrasent les informations qui restent sur les disques physiques.
- **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.
- **Chiffrer le disque virtuel** : chiffre le disque virtuel. Si le contrôleur est doté de capacités de chiffrement, vous pouvez créer, modifier ou supprimer les clés de sécurité.

  REMARQUE : L'option **Chiffrer le disque virtuel** est disponible uniquement si le disque virtuel est créé à l'aide de disques à chiffrement automatique (SED).
- **Gérer les disques de secours dédiés** : attribue ou annule l'attribution d'un disque physique en tant que disque de secours dédié. Seuls les disques de secours dédiés valides s'affichent. S'il n'y a pas de disques de secours dédiés valides, cette section ne s'affiche pas dans le menu déroulant.

Pour plus d'informations sur ces options, voir l'*aide en ligne d'iDAC*.

4. Depuis le menu déroulant **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.

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 des contrôleurs

Vous pouvez effectuer les tâches suivantes pour les contrôleurs :
- Configurer les propriétés du contrôleur
- Importer ou importer automatiquement une configuration étrangère
- Effacer une configuration étrangère
- Réinitialiser la configuration d'un contrôleur
- Créer, modifier ou supprimer des clés de sécurité

Concepts associés

Configuration des propriétés du contrôleur , page 217
Importation ou importation automatique d'une configuration étrangère , page 220
Suppression d'une configuration étrangère , page 221
Réinitialisation de la configuration d'un contrôleur , page 222
Contrôleurs pris en charge , page 204
Récapitulatif des fonctions prises en charge pour les périphériques de stockage , page 205
Conversion d'un disque physique au mode RAID ou non RAID , page 210

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 cohérence
- Mode de recopie
- Mode d'équilibrage de charge
- Taux de vérification de 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

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 des données.

La lecture cohérente n'est pas exécutée sur un disque physique dans les cas suivants :

- 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 de mode Patrol Read telles que **Start (Démarrer)** et **Stop (Arrêter)** ne sont pas prises en charge s'il n'y a pas de disques virtuels disponibles dans le contrôleur. Bien que vous puissiez appeler les opérations avec succès à l'aide des interfaces de l'iDRAC, les opérations échoueront lorsque la tâche associée sera démarrée.

Équilibrage de charge

La propriété d'équilibrage de la charge permet d'utiliser automatiquement à la fois les ports ou les connecteurs du contrôleur raccordés à la même enceinte pour acheminer les requêtes d'E/S. Cette propriété n'est disponible que pour les contrôleurs de stockage SAS.

Taux d'initialisation en arrière-plan (BGI)

L'initialisation en arrière-plan d'un disque virtuel redondant sur les contrôleurs PERC 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 qu'il maintienne les données redondantes et améliore les performances d'écriture. Par exemple, une fois l'initialisation en arrière-plan d'un disque virtuel RAID 5 terminée, les informations de parité sont initialisées. Une fois l'initialisation en arrière-plan d'un disque virtuel RAID 1 terminée, les disques physiques sont mis en miroir.

Le processus d'initialisation en arrière-plan aide le contrôleur à identifier et corriger les problèmes de données redondantes qui pourraient surgir ultérieurement. De ce point de vue, le processus d'initialisation en arrière-plan est similaire à une vérification de cohérence. Vous devriez laisser l'initialisation en arrière-plan se terminer. Si vous l'annulez, elle redémarrera automatiquement dans les 5 minutes qui suivront. Il est possible d'effectuer certains processus, tels que des opérations de lecture et d'écriture, pendant l'initialisation en arrière-plan. D'autres processus, tels que la création d'un disque virtuel, ne peuvent pas s'exécuter en même temps qu'une initialisation en arrière-plan. Ces processus annulent l'initialisation en arrière-plan.

Le taux d'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 0 %, l'initialisation en arrière-plan a le niveau de priorité le plus bas sur le contrôleur, prend le plus de temps à se terminer et a l'impact le moins important sur les performances du système. Une initialisation en arrière-plan d'un taux de 0 % ne signifie pas que le processus est arrêté ou interrompu. À 100 %, l'initialisation en arrière-plan a le niveau de priorité le plus élevé du contrôleur. Sa durée est réduite et il s'agit de la configuration ayant le plus d'impact sur les performances du système.

Vérifier la cohérence

La tâche de vérification de la cohérence vérifie l'exactitude des informations (de parité) redondantes. Cette tâche s'applique uniquement aux disques virtuels redondants. Si nécessaire, l'opération de vérification de la cohérence reconstruit les données redondantes. Si un disque virtuel est en état de Redondance en échec, l'exécution d'une vérification de cohérence peut rétablir l'état Prêt du disque virtuel.

Le taux de vérification de cohérence, configurable entre 0 et 100 %, représente le pourcentage des ressources système dédiées à l'exécution de la tâche de vérification de cohérence. À 0 %, la vérification de la cohérence a le niveau de priorité le plus bas sur le contrôleur, prend le plus de temps à se terminer et a l'impact le moins important sur la performance du système. Une vérification de la cohérence d'un taux de 0 % ne signifie pas que le processus est arrêté ou interrompu. À 100 %, la vérification de la cohérence a le niveau de priorité le plus élevé du contrôleur. Sa durée est réduite et il s'agit de la configuration ayant le plus d'impact sur les performances du système.

Créez ou modifiez les clés de sécurité

Lors de la configuration des propriétés du contrôleur, vous pouvez créer ou modifier les clés de sécurité. Le contrôleur utilise la clé de chiffrement pour verrouiller ou déverrouiller l'accès au disque SED. Vous ne pouvez créer qu'une seule clé de chiffrement pour chaque contrôleur doté de la capacité de chiffrement. La clé de sécurité est gérée à l'aide de fonction LKM (Local Key Management, Gestion de clés locale). LKM sert à générer l'ID de clé et le mot de passe ou la clé nécessaire pour sécuriser le disque virtuel. Si vous utilisez le Gestionnaire de clés local (LKM), vous devez créer la clé de chiffrement en spécifiant l'Identifiant de clé de chiffrement et la Phrase de passe.

Cette tâche n'est pas prise en charge sur les contrôleurs matériels PERC s'exécutant en mode HBA .

Si vous créez la clé de sécurité en mode Ajouter à l'opération en attente et qu'une tâche n'est pas créée, puis que vous supprimez la clé de sécurité, l'opération en attente de création de clé de sécurité est désactivée.

Configuration des propriétés des contrôleurs à l'aide de l'interface Web

1. Dans l'interface Web iDRAC, allez à **Présentation** > **Stockage** > **Contrôleurs** > **Configuration**.
   La page **Configurer les contrôleurs** s'affiche.
2. Dans la section **Configurer les propriétés du contrôleur**, dans le menu déroulant **Contrôleurs**, sélectionnez le contrôleur que vous voulez configurer.
3. Spécifiez les informations requises pour les différentes propriétés.

   La colonne **Valeur actuelle** affiche les valeurs existantes de chaque propriété. Vous pouvez modifier cette valeur en sélectionnant l'option dans le menu déroulant **Action** pour chaque propriété.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
4. Depuis le menu déroulant **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.

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 de mode Patrol Read telles que Start (Démarrer) et Stop (Arrêter) ne sont pas prises en charge s'il n'y a pas de disques virtuels disponibles dans le contrôleur. Bien que vous puissiez appeler les opérations avec succès à l'aide des interfaces de l'iDRAC, les opérations échoueront lorsque la tâche associée sera démarrée.

- 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 défiées à l'exécution d'une vérification de cohérence sur un disque virtuel redondant, utilisez l'objet **Storage.Controller.CheckConsistencyRate**.
- Pour spécifier le pourcentage des ressources du contrôleur dédiées à la reconstruction d'un disque en échec, utilisez l'objet **Storage.Controller.RebuildRate**
- Pour spécifier le pourcentage des 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 des 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>
```

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 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 contient uniquement un côté d'un miroir dans un disque virtuel RAID 1, le disque virtuel est alors à l'état Dégradé et peut être importé. En revanche, si la configuration étrangère ne contient qu'un seul disque physique qui avait été initialement configuré comme RAID 5 à l'aide de trois disques physiques, le disque virtuel RAID 5 est en 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 comme 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.

Si des configurations étrangères verrouillées à l'aide du LKM (Local Key Manager) sont détectées, l'opération d'importation de configuration étrangère n'est pas possible dans cette version d'iDRAC. Vous devez déverrouiller les disques en appuyant sur les touches CTRL+R et poursuivre l'importation de la configuration étrangère à partir de l'iDRAC.

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 : La tâche Importer la configuration étrangère importe tous les disques virtuels résidant sur les 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 de configurations étrangères sans exiger l'interaction entre les utilisateurs. L'option Importation automatique peut être activée ou désactivée. Si elle est activée, le contrôleur PERC peut importer automatiquement toute configuration étrangère détectée sans intervention manuelle. Si elle est désactivée, le contrôleur PERC n'importe automatiquement aucune configuration étrangère.

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 pourrait 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 lue et celui où l'importation réelle est effectuée. L'importation étrangère ne se produit que sur les lecteurs portant l'état Unconfigured Good (Non configuré - en bon état).
- Les lecteurs défectueux ou hors ligne ne peuvent pas être importés.
- Le micrologiciel ne vous permet pas d'importer plus de huit configurations étrangères.

Importation d'une configuration étrangère à l'aide de l'interface Web

Pour importer la configuration étrangère :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Stockage** > **Contrôleurs** > **Configuration**.
   La page **Configurer les contrôleurs** s'affiche.
2. Dans la section **Configuration étrangère**, dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur que vous voulez configurer.
3. Depuis le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez effectuer l'importation.
4. Cliquez sur **Importer la configuration étrangère**.

   La configuration est importée en fonction du mode de fonctionnement sélectionné.

   Pour importer automatiquement les configurations étrangères, dans la section **Configurer les propriétés du contrôleur**, activez l'option **Importation étrangère optimisée de configuration étrangère**, sélectionnez l'option **Appliquer le mode de fonctionnement**, puis cliquez sur **Appliquer**.

   REMARQUE : Vous devez redémarrer le système à froid après avoir activé l'option **Importation automatique optimisée de configurations étrangères** pour que les configurations étrangères prennent effet. Si un démarrage à chaud est effectué sur l'importation automatique, réalisez un racreset pour redémarrer le contrôleur iDRAC et voir ainsi les lecteurs importés dans iDRAC.

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**.

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 savoir si un disque physique précédemment utilisé contient ou non une configuration étrangère (disque virtuel) en vérifiant son état. Si l'état du disque physique est étranger, celui-ci contient alors la totalité ou une partie d'un disque virtuel. Vous pouvez effacer ou supprimer les informations du disque virtuel des disques physiques récemment raccordés.

L'opération Supprimer 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 peut être 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 qui ne peut pas être importée, vous pouvez utiliser l'option Supprimer une configuration étrangère pour supprimer les données étrangères 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 **Présentation** > **Stockage** > **Contrôleurs** > **Configuration**.
   La page **Configurer les contrôleurs** s'affiche.
2. Dans la section **Configuration étrangère**, dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur dont vous souhaitez effacer la configuration étrangère.
3. Dans le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez le moment auquel vous souhaitez effacer les données.
4. Cliquez sur **Effacer**.

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 disques virtuels et désattribue tous les disques de secours du contrôleur. Cela ne supprime que les disques de la configuration et n'efface aucune autre donnée. La réinitialisation de la configuration ne supprime pas de configurations étrangères. Le support en temps réel de cette fonction est uniquement disponible dans le micrologiciel PERC 9.1. La réinitialisation de la configuration n'efface pas de données. Vous pouvez recréer exactement la même configuration sans opération d'initialisation, qui peut entraîner la récupération des données. Vous devez disposer de privilèges de contrôle du serveur.

REMARQUE : La réinitialisation de la configuration du contrôleur ne supprime pas les configurations étrangères. Pour supprimer une configuration étrangère, effectuez l'opération Supprimer 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 iDRAC, accédez à **Présentation** > **Stockage** > **Contrôleurs** > **Dépannage**.
   La page **Dépannage des contrôleurs** s'affiche.
2. Dans le menu déroulant **Actions**, sélectionnez l'option **Réinitialiser la configuration** pour un ou 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

Sur les contrôleurs PERC 9.1 et versions ultérieures, vous pouvez modifier la personnalité du contrôleur en passant du mode RAID à 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 de préparation et ne se produit pas en temps réel. Avant de modifier le mode du contrôleur de RAID à HBA, assurez-vous que :

- Le contrôleur RAID prend en charge le changement de mode de contrôleur. L'option de changement du mode de contrôleur n'est pas disponible sur les contrôleurs RAID où la personnalité 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 en état de défaillance doivent être supprimés.
- Toute clé de sécurité locale associée à des disques autocryptables (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.

REMARQUE : Assurez-vous qu'une licence CMC est disponible pour les chariots de stockage PERC FD33xS et FD33xD avant de modifier le mode du contrôleur. Pour plus d'informations sur la licence CMC pour les chariots de stockage, voir le *Dell Chassis Management Controller Version 1.2 for PowerEdge FX2/FX2s User's Guide* (Guide d'utilisation du Dell Chassis Management Controller Version 1.2 pour PowerEdge FX2/FX2s) disponible à l'adresse **dell.com/support/manuals**.

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, RACADM ou WSMAN :

- 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** attribut 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 ou WSMAN :

- 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 fichier xml d'exportation pour faire passer le mode du contrôleur à RAID, convertir les lecteurs en Prêts et 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 XML 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 à l'exportation xml qui est modifié pour changer le mode du contrôleur à RAID, et que vous essayez de créer un disque virtuel, la création de 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 iDRAC, cliquez sur **Présentation** > **Stockage** > **Contrôleurs**.
2. Dans la page **Contrôleurs**, cliquez sur **Installation** > **Mode Contrôleur**.
   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**.
   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 en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Opérations de l'adaptateur HBA SAS 12 Gbits/s

Les contrôleurs non RAID sont les adaptateurs HBA ne disposant pas de certaines capacités RAID. Ils ne prennent pas en charge les disques virtuels.

L'interface iDRAC prend uniquement en charge les contrôleurs HBA SAS 12 Gbits/s et le contrôleur interne HBA330 dans cette version.

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 micrologiciel des boîtiers au dos du contrôleur HBA SAS 12 Gbits/s (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 :

- Vous devez effectuer l'opération Collect System Inventory On Reboot (CSIOR) avant de faire l'inventaire ou de surveiller les contrôleurs non RAID.
- Redémarrer le système après avoir effectué une mise à niveau du micrologiciel.
- La surveillance en temps réel des lecteurs SMART et des capteurs de boîtier SES est effectuée uniquement pour les contrôleurs HBA SAS 12 Gbits/s et les contrôleurs internes HBA330.

REMARQUE : Au cours du démarrage à chaud, il peut y avoir des journaux LC pour le disque PDR8 inséré. Cela est dû au fait que l'adaptateur HBA envoie des événements du disque inséré à l'iDRAC en raison du chargement et du déchargement du pilote HBA.

Concepts associés

Inventaire et surveillance des périphériques de stockage , page 207
Affichage de l'inventaire du système , page 106
Mise à jour du micrologiciel de périphérique , page 64
Surveillance de l'analyse de la prédiction d'échec sur des disques , page 224
Clignotement ou annulation du clignotement des LED des composants , page 236

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 qui prédit les échecs sur chaque disque et envoie des alertes si un échec de disque est prévu. Les contrôleurs vérifient si les disques physiques risquent d'échouer et, le cas échéant, transmettent ces informations à l'iDRAC. L'iDRAC journalise immédiatement une alerte.

Opérations de contrôleur en mode non RAID - 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 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 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.
- Effacez une 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 tâche sur le contrôleur suivant.
- Planifier plusieurs tâches à exécuter ultérieurement à l'aide des options de planification.

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 de niveau professionnel. Le périphérique SSD PCIe comprend une technologie flash NAND SLC (Single Level Cell) et MLC (Multi-Level Cell) associée à une interface ultra-rapide conforme à PCIe 2.0 ou PCIe 3.0. IDRAC 2.20.20.20 et les versions ultérieures prennent en charge les cartes PCIe SSD mi-hauteur demi-longueur (HHHL) sur les serveurs en rack et en tour Dell PowerEdge de 13e génération et les serveurs Dell PowerEdge R920. La carte SSD HHHL peut être branchée directement dans l'emplacement PCI dans les serveurs qui ne disposent pas de fonds de paniers prenant en charge les SSD PCIe. Vous pouvez également utiliser ces cartes prises en charge sur des serveurs avec fonds de panier pris en charge.

Utiliser les interfaces iDRAC, vous pouvez afficher et configurer les SSD PCIe NVMe.

Fonctionnalités clé du lecteur SSD PCIe :

- Capacité d'enfichage à chaud
- Périphérique hautes performance

Le sous-système SSD PCIe comprend le fond de panier, une carte d'extension PCIe connectée au fond de panier du système et offre une connectivité PCIe pour jusqu'à quatre ou huit SSD PCIe à l'avant du châssis et les SSD PCIe.

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 du voyant LED du périphérique

Vous pouvez effectuer les opérations suivantes pour les SSD HHHL :

- Inventaire et surveillance en temps réel du disque SSD HHHL dans le serveur
- Rapport d'état du disque tel que En ligne, Échec, et Hors ligne
- 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

REMARQUE : La capacité d'enfichage à chaud, la préparation au retrait et le clignotement ou l'arrêt du clignotement du voyant LED du périphérique ne s'appliquent pas aux périphériques SSD PCIe HHHL.

Concepts associés

Inventaire et surveillance de SSD PCIe , page 226
Préparation au retrait d'un SSD PCIe , page 226
Effacement des données d'un périphérique SSD PCIe , page 228

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

    Si le système est équipé d'un fond de panier PCIe dédié, deux FQDD sont affichés. Un FQDD concerne les disques normaux et l'autre les SSD. Si le fond de panier est partagé (universel), un seul FQDD s'affiche.
- 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 iDRAC, accédez à **Présentation** > **Stockage** > **Disques physiques**. La page **Propriétés** s'affiche. Dans le cas des SSD PCIe, la colonne **Nom** affiche **PCIe SSD**. Développez-la pour afficher les propriétés.

Inventaire et surveillance de SSD PCIe à l'aide de RACADM

Utilisez la commande `racadm storage get controllers:<PcieSSD controller FQDD>` pour dresser un inventaire et surveiller les SSD PCIe.

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 iDRAC*, disponible sur **dell.com/idracmanuals**.

Préparation au retrait d'un SSD PCIe

Les SSD PCIe prennent en charge l'échange à chaud séquentiel, vous permettant d'ajouter ou supprimer un périphérique sans interrompre ou réamorcer le système dans lequel les périphériques sont installés. Pour éviter de perdre des données, vous devez utiliser la tâche Prepare to Remove (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 pris en charge exécutant un système d'exploitation pris en charge. Pour être sûr que vous disposez de la bonne configuration matérielle pour votre périphérique SSD PCIe, consultez le Owner's Manual (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.

REMARQUE : L'opération de préparation au retrait est prise en charge sur les systèmes avec ESXi 6.0 avec iDRAC Service Module version 2.1 ou plus récente.

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 effectué l'opération de préparation au retrait :

- Le SSD PCIe clignote et suit la séquence de LED signifiant Prêt à être retiré.
- 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 iDRAC, accédez à **Présentation** > **Stockage** > **Disques physiques** > **Configuration**.
   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 que iSM est installé et en cours d'exécution pour effectuer l'opération `Préparer au retrait`.
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 périphériques SSD PCIe, seule l'option **Appliquer maintenant** est disponible. Cette opération n'est pas prise en charge en mode intermédiaire.
5. Cliquez sur **Appliquer**.

   Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué apparaît. De plus, l'ID du message et l'action de réponse recommandée s'affiche.

   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 réussit et la création de tâche n'est pas exécutée avec succès, 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 référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Effacement des données d'un périphérique SSD PCIe

La fonction Secure Erase (Effacement sécurisé) efface définitivement toutes les données présentes sur le disque. L'exécution d'un effacement cryptographique sur un SSD PCIe écrase tous les blocs et entraîne la perte définitive de toutes les données du SSD PCIe. Au cours de l'effacement cryptographique, l'hôte ne peut pas accéder au SSD PCIe. Les modifications sont appliquées après le redémarrage du système.

Si le système se réinitialise ou subit une panne de courant lors de l'effacement cryptographique, l'opération est annulée. Vous devez redémarrer le système et relancer 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 effacé, le disque s'affiche dans le système d'exploitation comme étant en ligne, mais non initialisé. Vous devez réinitialiser et reformater le disque pour pouvoir l'utiliser à nouveau.
- Une fois un SSD PCIe enfiché à chaud, il peut mettre quelques secondes à s'afficher dans l'interface web.
- La fonction d'effacement sécurisé n'est pas prise en charge pour les disques SSD PCIe branchés à chaud

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 iDRAC, accédez à **Présentation** > **Stockage** > **Disques physiques** > **Configuration**.
   La page **Sélectionner des 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 sécurisé** pour un ou disques SSD PCIe.

   Si vous avez sélectionné **Effacement sécurisé** 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** : sélectionnez cette option pour appliquer les actions au cours du prochain redémarrage du système. Il s'agit de l'option par défaut pour les contrôleurs PERC 8.
   - **À l'heure programmée)** : sélectionnez cette option pour appliquer les actions à un jour et à une heure de début planifiés :
     - **Heure de début** et **Heure de fin** : cliquez sur les icônes de calendrier et sélectionnez les jours. Dans les menus déroulants, sélectionnez l'heure. Cette action s'applique entre les heures de début et 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)

       REMARQUE : Pour les contrôleurs PERC 8 ou version antérieure, **Arrêt normal** est la valeur par défaut. Pour les contrôleurs PERC 9, **Pas de redémarrage (Redémarrage manuel du système)** est l'option par défaut.
5. Cliquez sur **Appliquer**.

   Si la tâche n'est pas créée, un message indiquant que la création de la tâche a échoué apparaît. De plus, l'ID du message et l'action de réponse recommandée s'affiche.

   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 des tâches** pour afficher l'avancement de la tâche dans la page File d'attente des tâches.

   Si l'opération en attente n'est pas créée, un message d'erreur s'affiche. Si l'opération en attente réussit et la création de tâche n'est pas exécutée avec succès, 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 le travail cible après avoir exécuté la commande `secureerase` :

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

Pour rechercher l'ID de travail renvoyé :

```
racadm jobqueue view -i <job ID>
```

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

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

Concepts associés

Récapitulatif des fonctions prises en charge pour les périphériques de stockage , page 205
Boîtiers pris en charge , page 205
Configuration du mode du fond de panier , page 229
Affichage des logements universels , page 232
Définition du mode SGPIO , page 232

Configuration du mode du fond de panier

Les serveurs Dell PowerEdge de 13e génération prennent en charge une nouvelle topologie de stockage interne, dans laquelle deux contrôleurs de stockage (PERC) peuvent être connectés à un ensemble de disques internes par le biais d'un même extenseur. Cette configuration est utilisée pour le mode hautes performances sans basculement ou pour la fonctionnalité de haute disponibilité (HA). L'extenseur divise la matrice de disques internes entre les deux contrôleurs de stockage. Dans ce mode, la création d'un disque virtuel affiche uniquement les disques connectés à un contrôleur particulier. Aucune licence n'est nécessaire pour utiliser cette fonctionnalité. Celle-ci n'est prise en charge que sur certains systèmes.

Le fond de panier prend en charge les modes suivants :

- Mode unifié (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 divisé : un contrôleur a accès aux 12 premiers disques et le second contrôleur a accès aux 12 derniers disques. Les lecteurs connectés au premier contrôleur sont numérotés de 0 à 11, tandis que les disques durs connectés au second contrôleur sont numérotés de 12 à 23.
- Mode divisé 4:20 : un contrôleur a accès aux 4 premiers disques et le second contrôleur a accès aux 20 derniers disques. Les lecteurs connectés au premier contrôleur sont numérotés de 0 à 3, tandis que les disques durs connectés au second contrôleur sont numérotés de 4 à 23.
- Mode divisé 8:16 : un contrôleur a accès aux 8 premiers disques et le second contrôleur a accès aux 16 derniers disques. Les lecteurs connectés au premier contrôleur sont numérotés de 0 à 7, tandis que les disques durs connectés au second contrôleur sont numérotés de 8 à 23.
- Mode divisé 16:8 : un contrôleur a accès aux 16 premiers disques et le second contrôleur a accès aux 8 derniers disques. Les lecteurs connectés au premier contrôleur sont numérotés de 0 à 15, tandis que les disques durs connectés au second contrôleur sont numérotés de 16 à 23.
- Mode divisé 20:4 : un contrôleur a accès aux 20 premiers disques et le second contrôleur a accès aux 4 derniers disques. Les lecteurs connectés au premier contrôleur sont numérotés de 0 à 19, tandis que les disques durs connectés au second contrôleur sont numérotés de 20 à 23.

- Informations non disponibles : les informations de contrôleur ne sont pas disponibles.

iDRAC autorise le mode divisé si l'extenseur a la capacité de prendre en charge la configuration. Veillez à activer ce mode avant de procéder à l'installation du deuxième contrôleur. iDRAC effectue une vérification de capacité d'extension avant d'autoriser la configuration de ce mode et ne vérifie pas si le deuxième contrôleur PERC est présent.

Pour modifier le paramètre, vous devez disposer des privilèges de contrôle du serveur.

Si d'autres opérations RAID sont en état d'attente ou si des tâches RAID sont planifiées, vous ne pouvez pas modifier le mode du fond de panier. De la même façon, 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.
- 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 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 iDRAC, allez à **Présentation** > **Stockage** > **Boîtiers** > **Configuration**.
   La page **Configuration du boîtier** s'affiche.
2. Dans le menu déroulant **Contrôleur**, sélectionnez le contrôleur pour configurer les enceintes qui lui sont associées.
3. Dans la colonne **Valeur**, sélectionnez le mode pour le boîtier ou le fond de panier requis :
   - Mode unifié
   - Mode fractionné
   - Mode fractionné 4:20
   - Mode fractionné 8:16
   - Mode fractionné 16:8
   - Mode fractionné 20:4
   - Informations non disponibles
4. Dans le menu déroulant **Appliquer le mode de fonctionnement**, sélectionnez **Appliquer maintenant** pour appliquer les actions immédiatement, puis cliquez sur **Appliquer**.
   Un ID de tâche est créé.
5. Accédez à la page **File d'attente des tâches** et vérifiez que la tâche affiche l'état Terminé.
6. Effectuez un cycle d'alimentation sur le système pour que la configuration soit appliquée.

Configuration du boîtier à l'aide de RACADM

Pour configurer le boîtier ou le fond de panier, utilisez la commande `set` avec les objets en **BackplaneMode**.

Par exemple, pour définir l'attribut BackplaneMode sur le mode partagé :

1. Exécutez la commande suivante pour afficher le mode backplane 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` est 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 le POST et le CSIOR, tapez la commande suivante pour vérifier le `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**.

Affichage des logements universels

Certains fonds de panier de serveurs PowerEdge de 13e génération PowerEdge prennent en charge la coexistence de SSD SAS/SATA et PCIe dans le même logement. Ces logements sont appelés logements universels et ils sont câblés vers le contrôleur de stockage principal (PERC) et vers une carte d'extenseur PCIe. Le micrologiciel du fond de panier fournit des informations aux logements qui prennent en charge cette fonctionnalité. Le fond de panier prend en charge des disques SAS/SATA ou des SSD PCIe. Normalement, les quatre logements à numéros les plus élevés sont universels. Par exemple, dans un fond de panier universel à 24 logements, les logements 0 à 19 ne prennent en charge que des disques SAS/SATA tandis que les logements 20 à 23 prennent en charge des SSD, soit SAS/SATA, soit PCIe.

L'état cumulé d'intégrité du boîtier fournit l'état de l'intégrité de tous les lecteurs qu'il contient. Le lien Boîtier de la page **Topologie** affiche l'ensemble des informations relatives au boîtier, quel que soit le contrôleur auquel il est associé. Comme deux contrôleurs de stockage (PERC et extenseur PCIe) peuvent être connectés au même fond de panier, seul le fond de panier associé au contrôleur PERC s'affiche dans la page **Inventaire du système**.

Dans la page **Stockage** > **Boîtiers** > **Propriétés**, la section **Présentation des disques physiques** affiche les éléments suivants :

- **Logement vide** : si un logement est vide.
- **Compatible PCIe** : s'il n'y a pas de logements compatibles PCIe, cette colonne n'est pas affichée.
- **Protocole de bus** : s'il s'agit d'un fond de panier universel doté d'un disque SSD PCIe installé dans l'un des emplacements, cette colonne affiche **PCIe**.
- **Disque de secours** : cette colonne ne s'applique pas au SSD PCIe.

REMARQUE : Le remplacement à chaud est pris en charge par les logements universels. Si vous souhaitez retirer un disque SSD PCIe et le remplacer par un disque SAS/SATA, veillez d'abord à effectuer la tâche de préparation au retrait pour le disque SSD PCIe. Si vous n'effectuez pas cette tâche, le système d'exploitation hôte peut rencontrer des problèmes (écran bleu, panique du noyau, etc.).

Définition du mode SGPIO

Le contrôleur de stockage peut se connecter au fond de panier en mode I2C (paramètre par défaut des fonds de panier Dell) ou en mode SGPIO (Serial General Purpose Input/Output). Cette connexion est nécessaire pour le clignotement des voyants LED sur les lecteurs. Les contrôleurs PERC et fond de panier Dell prennent en charge ces modes. Pour prendre en charge certains adaptateurs de canal, le mode du fond de panier doit être changé au mode SGPIO.

Le mode SGPIO est pris en charge uniquement par les fonds de panier passifs. Il n'est pas pris en charge par les fonds de panier d'extenseur ou passifs en aval. Le micrologiciel du fond de panier fournit des informations sur sa capacité, son état actuel et l'état demandé.

Suite à l'opération d'effacement de LC ou de restauration des valeurs par défaut d'iDRAC, le mode SGPIO est réinitialisé à l'état désactivé. Il compare le paramètre iDRAC avec celui du fond de panier. Si le fond de panier est défini sur le mode SGPIO, iDRAC change son paramètre pour le faire correspondre à celui 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**.

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. C'est-à-dire, spécifiez le moment auquel 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 :
   - **Présentation** > **Stockage** > **Disques physiques** > **Configuration**.
   - **Présentation** > **Stockage** > **Disques virtuels** > **Créer**
   - **Présentation** > **Stockage** > **Disques virtuels** > **Gérer**
   - **Présentation** > **Stockage** > **Contrôleurs** > **Configurer**
   - **Présentation** > **Stockage** > **Contrôleurs** > **Dépannage**
   - **Présentation** > **Stockage** > **Boîtiers** > **Configuration**
   - **Présentation** > **Stockage** > **Opérations en attente**
2. Sélectionnez l'une des options suivantes du menu déroulant **Appliquer le mode de fonctionnement** :
   - **Appliquer maintenant** : sélectionnez cette option pour appliquer les paramètres immédiatement. Cette option est disponible pour les contrôleurs PERC 9 uniquement. S'il existe des tâches à terminer, cette option est grisée. Cette tâche prend au moins 2 minutes.
   - **Au prochain redémarrage** : sélectionnez cette option pour appliquer les paramètres au cours du prochain redémarrage du système. Il s'agit de l'option par défaut pour les contrôleurs PERC 8.
   - **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 jours. Dans les menus déroulants, sélectionnez l'heure. Les paramètres s'appliquent entre les heures de début et 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)

       REMARQUE : Pour les contrôleurs PERC 8 ou version antérieure, **Arrêt normal** est la valeur par défaut. Pour les contrôleurs PERC 9, **Pas de redémarrage (Redémarrage manuel du système)** est l'option par défaut.
   - **Ajouter aux opérations en attente** : sélectionnez cette option pour créer une opération en attente pour appliquer les paramètres. Vous pouvez afficher tous les opérations en attente d'un contrôleur dans la page **Présentation** > **Stockage** > **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 en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Affichage et application des opérations en attente

Utilisez cette page pour 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 individuellement les opérations en attente.

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 SSD PCIe, la tâche est créée sur un disque SSD PCIe et non sur l'extenseur PCIe.

Affichage, application ou suppression des opérations en attente à l'aide de l'interface Web

1. Dans l'interface Web iDRAC, allez à **Présentation** > **Stockage** > **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 cryptage de disques virtuels. Toutefois, elles ne sont pas affichées dans la page **Opérations en attente** ni 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 :
   - **Appliquer maintenant** : sélectionnez cette option pour enregistrer toutes les opérations immédiatement. Cette option est disponible pour les contrôleurs PERC 9 équipés de la dernière version de micrologiciel.
   - **Au prochain redémarrage** : sélectionnez cette option pour valider toutes les opérations au cours du prochain redémarrage du système. Il s'agit de l'option par défaut pour les contrôleurs PERC 8. Cette option est uniquement applicable pour PERC 8 et les versions ultérieures.
   - **À l'heure programmée** : sélectionnez cette option pour valider les opérations à un jour et à une heure spécifiés. Cette option est uniquement applicable pour PERC 8 et les versions ultérieures.
     - **Heure de début** et **Heure de fin** : cliquez sur les icônes de calendrier et sélectionnez les jours. Dans les menus déroulants, sélectionnez l'heure. Cette action s'applique entre les heures de début et 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)

       REMARQUE : Pour les contrôleurs PERC 8 ou version antérieure, **Arrêt normal** est la valeur par défaut. Pour les contrôleurs PERC 9, **Pas de redémarrage (Redémarrage manuel du système)** est l'option par défaut.
5. Si la tâche de validation n'est pas créée, un message indiquant que la création de la tâche a échoué apparaît. De plus, l'ID du message et l'action de réponse recommandée s'affichent.

6. Si la tâche de validation est créée avec succès, un message indiquant que l'ID de tâche est créée pour le contrôleur sélectionné s'affiche. Cliquez sur **File d'attente des tâches** pour afficher l'avancement de la tâche dans la page **File d'attente des tâches**.

   Si la suppression d'une configuration étrangère, l'importation d'une configuration étrangère, des opérations de clé de sécurité ou des opérations de cryptage de disque virtuel sont en attente et s'il s'agit des seules opérations en attente, vous ne pouvez pas créer une tâche à partir de la page **Opérations en attente**. Vous devez effectuer une autre opération de configuration de stockage ou utiliser RACADM ou WSMAN pour créer la tâche de configuration nécessaire sur le contrôleur requis.

   Vous ne pouvez pas afficher ou effacer les opérations en attente pour les SSD PCIe dans la page **Opérations en attente**. Utilisez la commande racadm pour effacer les opérations en attente des 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 en savoir plus, 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 de 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 de 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 pour activer ou désactiver le clignotement d'un voyant.

Le contrôleur doit prendre en charge la configuration en temps réel. Le support en temps réel de cette fonction est disponible uniquement dans le micrologiciel PERC 9.1 et les 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 :
   - **Présentation** > **Stockage** > **Identifier** : affiche la page **Identification des LED des composants**, où vous pouvez activer ou désactiver le clignotement des disques physiques, des disques virtuels et des SSD PCIe.
   - **Présentation** > **Stockage** > **Disques physiques** > **Identifier** : affiche la page **Identifier les disques physiques**, où vous pouvez activer ou désactiver le clignotement des disques physiques et des SSD PCIe.
   - **Présentation** > **Stockage** > **Disques virtuels** > **Identifier**: affiche la page **Identifier les disques physiques**, où vous pouvez activer ou désactiver le clignotement des disques virtuels.
2. Si vous êtes sur la page **Identifier le LED de composant** :
   - Sélectionnez ou désélectionnez toutes les DEL des composants : sélectionnez l'option **Sélectionner/Désélectionner tout**, puis cliquez sur **Clignotement** pour démarrer le clignotement des DEL des composants. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des DEL des composants.
   - Sélectionnez ou désélectionnez des DEL de composants individuels : sélectionnez une ou plusieurs DEL de composants et cliquez sur **Clignotement** pour démarrer le clignotement de la/des DEL du/des composant(s) sélectionné(s). De la même façon, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des DEL des composants.
3. Si vous êtes sur la page **Identifier les disques physiques** :

- Sélectionnez ou désélectionnez tous les lecteurs de disque physique ou SSD PCIe : sélectionnez l'option **Sélectionner/ Désélectionner tout**, puis cliquez sur **Clignotement** pour démarrer le clignotement des LED sur tous les lecteurs de disque physique et les 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 DEL.

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 DEL de l'ensemble des disques virtuels. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des DEL.
   - Sélectionnez ou désélectionnez des disques virtuels : sélectionnez un ou plusieurs disques virtuels et cliquez sur **Clignotement** pour démarrer le clignotement des DEL des disques virtuels. De même, cliquez sur **Arrêter le clignotement** pour arrêter le clignotement des DEL.

   Si l'opération d'activation ou de désactivation du clignotement échoue, un message d'erreur s'affiche.

Clignotement ou annulation 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**.

14

Configuration et utilisation de la console virtuelle

Vous pouvez utiliser la console virtuelle pour gérer un système distant en utilisant le clavier, la vidéo et la souris sur la station de gestion pour contrôler les périphériques correspondants sur un serveur géré. Il s'agit d'une fonction disponible sous licence pour les serveurs en rack et en tour. Elle est disponible par défaut dans les serveurs lames.

Les principales fonctions sont les suivantes :

- Vous pouvez avoir jusqu'à six sessions de console virtuelle simultanées. Toutes les sessions voient la même console de serveur géré simultanément.
- Vous pouvez lancer la console virtuelle dans un navigateur web pris en charge à l'aide du plug-in Java, ActiveX ou HTML5.
- Lorsque vous ouvrez une session de console virtuelle, le serveur géré n'indique pas que la console a été redirigée.
- Vous pouvez ouvrir plusieurs sessions de console virtuelle depuis une même station de gestion sur un ou plusieurs systèmes gérés simultanément.
- Vous ne pouvez pas ouvrir deux sessions de console virtuelle depuis la station de gestion vers le serveur géré en utilisant le même plug-in.
- Si un second utilisateur demande une session de console virtuelle, 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 deuxième utilisateur est averti qu'un autre utilisateur contrôle la session. 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. Lorsque deux sessions sont actives simultanément, le premier utilisateur voit un message dans l'angle supérieur droit de l'écran indiquant que le deuxième utilisateur a une session active. Si aucun des utilisateurs ne dispose de privilège de l'administrateur, le fait de quitter la session du premier utilisateur mettra fin automatiquement à celle du second.

REMARQUE : Pour plus d'informations sur la configuration de votre navigateur pour accéder à la console virtuelle, voir Configuration des navigateurs Web pour utiliser la console virtuelle , page 60.

REMARQUE : Lorsque la licence iDRAC expire ou est supprimée, la console virtuelle et les ports média virtuel sont automatiquement fermés, entraînant l'arrêt de toutes les sessions de console virtuelle et de média virtuel.

Concepts associés

Configuration des navigateurs Web pour utiliser la console virtuelle , page 60
Configuration de la console virtuelle , page 239
Lancement de la console virtuelle , page 240

Sujets :

- Résolutions d'écran prises en charge et taux de rafraîchissement correspondants
- Configuration de la console virtuelle
- Prévisualisation de la console virtuelle
- Lancement de la console virtuelle
- Utilisation du Visualiseur de console virtuelle

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 39. Résolutions d'écran prises en charge et taux de rafraîchissement correspondants

Résolution d'écran	Taux de rafraîchissement (Hz)
720 x 400	70
640 x 480	60, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1 024 x 768	60, 70, 72, 75, 85
1 280 x 1 024	60

Il est recommandé de configurer la résolution d'affichage minimale 1 280 x 1 024 sur le moniteur.

REMARQUE : Si vous avez une session de console virtuelle active et si un moniteur de plus faible résolution est connecté à la console virtuelle, la résolution de la console de serveur peut se réinitialiser si le serveur est sélectionné sur la console locale. Si le système fonctionne sous un système d'exploitation Linux, une console X11 peut ne pas être visible sur l'écran local. Appuyez sur <Ctrl><Alt><F1> à la console virtuelle iDRAC pour commuter Linux vers une console texte.

Configuration de la console virtuelle

Avant de configurer la console virtuelle, vérifiez que la station de gestion est configurée.

Vous pouvez configurer la console virtuelle à l'aide de l'interface Web iDRAC ou de l'interface de ligne de commande RACADM.

Concepts associés

Configuration des navigateurs Web pour utiliser la console virtuelle , page 60
Lancement de la console virtuelle , page 240

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 **Présentation générale** > **Serveur** > **Console virtuelle**. La page **Console Virtuelle** s'affiche.
2. Activez la console virtuelle et définissez les valeurs nécessaires. Pour plus d'information sur les options, voir l'*aide en ligne d'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 en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Prévisualisation de la console virtuelle

Avant de lancer la console virtuelle, vous pouvez prévisualiser son état sur la page **Système** > **Propriétés** > **Résumé du système**. La section de **Prévisualisation de la console virtuelle** contient une image indiquant l'état de la console virtuelle. L'image est actualisée toutes les 30 secondes. Il s'agit d'une fonction disponible sous licence.

REMARQUE : L'image de la console virtuelle est disponible uniquement si vous avez activé la console virtuelle.

Lancement de la console virtuelle

Vous pouvez lancer la console virtuelle à l'aide de l'interface Web d'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, vérifiez que :

- Vous disposez des privilèges d'administrateur.
- Un navigateur Web est configuré pour utiliser les plug-ins HTML5, Java ou ActiveX.
- Une bande passante de 1 Mo/s est disponible.

REMARQUE : Si le contrôleur vidéo intégré est désactivé dans le BIOS et si vous lancez la console virtuelle, le Virtual Console Viewer (visualiseur de la console virtuelle) sera vide.

Lorsque vous lancez la console virtuelle en utilisant un navigateur 32 bits ou 64 bits, utilisez HTML%, ou utilisez le plug-in requis (Java ou ActiveX) qui est disponible dans le navigateur respectif. Les paramètres Options Internet sont communs à tous les navigateurs

Lorsque vous lancez la console virtuelle en utilisant le plug-in Java, une erreur de compilation Java peut se produire. Pour l'éliminer, accédez à **Panneau de configuration Java** > **Général** > **Paramètres réseau**, puis sélectionnez **Connexion directe**.

Si la console virtuelle est configurée pour utiliser le plug-in ActiveX, elle peut ne pas démarrer la première fois. Ceci s'explique par le fait que la connexion réseau est lente et que le délai d'expiration des données d'identification (utilisées par la console virtuelle pour la connexion) est de deux minutes. Le délai de téléchargement du plug-in du client ActiveX peut dépasser ce délai. Une fois le plug-in téléchargé, vous pouvez lancer la console normalement.

Pour lancer la console virtuelle à l'aide du plug-in HTML5, vous devez désactiver le bloqueur de fenêtres publicitaires intempestives.

Concepts associés

Lancement de la console virtuelle à l'aide d'une URL , page 240
Configuration d'Internet Explorer pour qu'il utilise le plug-in HTML5 , page 61
Configuration du navigateur Web pour utiliser le plug-in Java , page 61
Configuration d'IE pour qu'il utilise le plug-in ActiveX , page 62
Lancement de la console virtuelle à l'aide de l'interface Web , page 240
Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX , page 241
Synchronisation des pointeurs de souris , page 243

Lancement de la console virtuelle à l'aide de l'interface Web

Vous pouvez lancer la console virtuelle des manières suivantes :

- Allez à **Présentation générale** > **Serveur** > **Console virtuelle**. La page **Console virtuelle** s'affiche. Cliquez sur **Lancer la console virtuelle**. Le **Visualiseur de console virtuelle** démarre.
- Allez à **Présentation générale** > **Serveur** > **Propriétés**. La page **Résumé du système** s'affiche. Dans la section **Prévisualisation de la console virtuelle**, cliquez sur **Lancer**. Le **Visualiseur de console virtuelle** démarre.

Le **Visualiseur de console virtuelle** affiche le bureau du système distant. Ce visualiseur permet de contrôler les fonctions de la souris et du clavier du système distant depuis la station de gestion.

Plusieurs boîtes de message peuvent s'afficher après le lancement de l'application. Pour interdire tout accès non autorisé à l'application, naviguez dans ces boîtes de message dans un délai de trois minutes pour éviter d'avoir à redémarrer l'application.

Si des fenêtres d'alerte de sécurité s'affichent lors du lancement du Visualiseur, cliquez sur Oui pour continuer.

Deux pointeurs de souris peuvent apparaître dans la fenêtre du visualiseur : un pour le serveur géré et un autre pour votre station de gestion. Pour synchroniser les curseurs, voir Synchronisation des pointeurs de souris.

Lancement de la console virtuelle à l'aide d'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 la connexion directe est désactivée et que la connexion locale, Active Directory, LDAP ou par carte à puce est activée, la page **Ouverture de session** correspondante s'affiche.
- Si la connexion directe est activée, le **Visualiseur de console virtuelle** s'ouvre et la page **Console virtuelle** s'affiche en arrière-plan.

REMARQUE : Internet Explorer prend en charge les ouvertures de session locales, Active Directory, LDAP, par carte à puce (SC) et par connexion directe. Firefox prend en charge les ouvertures de session locales, AD et par connexion directe sur le système d'exploitation Windows, et locales, Active Directory et LDAP sur les systèmes d'exploitation Linux.

REMARQUE : Si vous ne disposez pas des privilèges d'accès à la console virtuelle, cette URL lance Média Virtuel et non pas la console virtuelle.

Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX

Vous pouvez désactiver les messages d'avertissement lors du lancement de la console virtuelle ou du média virtuel en utilisant le plug-in Java.

1. Initialement, lorsque vous lancez la console virtuelle ou le média virtuel en utilisant le plug-in Java, l'invite pour vérifier l'éditeur s'affiche. Cliquez sur **Oui**.

   Un message d'avertissement de certificat s'affiche pour indiquer qu'un certificat de confiance est introuvable.

   REMARQUE : Si le certificat est trouvé dans le magasin de certificats du système d'exploitation ou s'il est détecté dans un emplacement d'utilisateur indiqué précédemment, ce message d'avertissement n'est pas affiché.

2. Cliquez sur **Continue** (Continuer).
   Le visualiseur de console virtuelle ou de média virtuel s'ouvre.

   REMARQUE : Le visualiseur du média virtuel est lancé si la console virtuelle est désactivée.

3. Dans le menu **Outils**, cliquez sur **Options de session**, puis sur l'onglet **Certificat**.
4. Cliquez sur **Rechercher le chemin**, spécifiez l'emplacement de stockage du certificat de l'utilisateur, cliquez sur **Appliquer**, puis sur **OK** et fermez le visualiseur.
5. Lancez la console virtuelle à nouveau.
6. Dans le message d'avertissement de certificat, sélectionnez l'option **Toujours faire confiance à ce certificat**, puis cliquez sur **Continuer**.
7. Quittez le visualiseur.
8. Lorsque vous relancez la console virtuelle, le message d'avertissement ne s'affiche pas.

Utilisation du Visualiseur de console virtuelle

Le visualiseur de la console virtuelle fournit différentes commandes telles que la synchronisation des souris, le facteur d'échelle de la console virtuelle, les options de messagerie, les macros de clavier, les actions d'alimentation, les périphériques de démarrage suivants et l'accès au média virtuel. Pour en savoir plus sur l'utilisation de ces fonctions, voir l'*aide en ligne d'iDRAC*.

REMARQUE : Si le serveur distant est hors tension, le message « Aucun signal » s'affiche.

La barre de titre du Visualiseur de console virtuelle contient le nom DNS ou l'adresse IP de l'iDRAC auquel vous êtes connecté depuis la station de gestion. Si iDRAC n'a pas de nom DNS, l'adresse IP est affichée. Le format est :

- Pour les serveurs en rack et de type tour :

  ```
  <DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>
  ```

- Pour les serveurs lames :

  ```
  <DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>
  ```

Il peut arriver que le Visualiseur de console virtuelle affiche une vidéo de mauvaise qualité. Ceci est dû à la lenteur de la connectivité réseau qui provoque une perte d'une ou de deux trames vidéo lorsque vous démarrez la session de console virtuelle. Pour transmettre toutes les trames vidéo et améliorer la qualité vidéo, procédez de l'une des manières suivantes :

- Dans la page **Résumé du système**, dans la section **Prévisualisation de la console virtuelle**, cliquez sur **Actualiser**.
- Dans **Visualiseur de console virtuelle**, dans l'onglet **Performances**, amenez le curseur sur **Qualité vidéo maximale**.

Console virtuelle HTML5

REMARQUE : La console virtuelle HTML est uniquement prise en charge sous Windows 10. Vous devez utiliser Internet Explorer 11 ou Google Chrome pour accéder à cette fonctionnalité.

REMARQUE : Pour accéder à la console virtuelle avec HTML5, vous devez vous assurer que le système client, le clavier cible, le système d'exploitation et le navigateur utilisent la même langue. Par exemple, ils doivent tous être en anglais (États-Unis) ou dans l'une des langues prises en charge.

Pour lancer la console virtuelle HTML5, vous devez activer la fonctionnalité de console virtuelle à partir de la page iDRAC Virtual Console (Console virtuelle d'iDRAC) et configurer l'option **Virtual Console Type (Type de console virtuelle)** sur HTML5.

Vous pouvez lancer la console virtuelle en tant que fenêtre contextuelle à l'aide de l'une des méthodes suivantes :

- À partir de la page d'accueil de l'iDRAC, cliquez sur le lien **Launch (Lancer)** disponible dans la session Console Preview (Prévisualisation de la console).
- À partir de la page iDRAC Virtual Console (Console virtuelle d'iDRAC), cliquez sur **Launch Virtual Console (Lancer la console virtuelle)**.
- Depuis la page de connexion au contrôleur iDRAC, tapez **https//<IP de l'iDRAC>/console**. Cette méthode est appelée Direct Launch (Lancement direct).

Les options de menu suivantes sont disponibles dans la console virtuelle HTML5 :

- Chat
- Clavier
- Capture d'écran
- Actualiser
- Plein écran
- Déconnecter le visualiseur
- Commande de la console
- Média virtuel

L'option **Pass all keystrokes to server (Envoyer toutes les frappes au serveur)** n'est pas prise en charge par la console virtuelle HTML5. Utilisez le clavier et les macros de clavier pour accéder à toutes les touches de fonction.

- Commande de la console : dispose des options de configuration suivantes :
  - Clavier
  - Macros de clavier
  - Format d'image
  - Mode tactile
  - Accélération de la souris
- Clavier : ce clavier utilise un code open source. La différence avec un clavier physique est que les touches numériques sont commutées en caractères spéciaux lorsque vous activez la touche **Caps Lock (Verr Maj)**. La fonction reste la même et le chiffre est entré si vous appuyez sur le caractère spécial lorsque la touche **Verr Maj** est activée.
- Macros de clavier : ces fonctions sont prises en charge par la console virtuelle HTML5 et s'affichent dans une liste déroulante. Cliquez sur **Apply (Appliquer)** pour appliquer la combinaison de touches sélectionnée sur le serveur.
  - Ctrl+Alt+Suppr
  - Alt+Tab
  - Alt+Échap
  - Ctrl+Échap
  - Alt+Espace
  - Alt+Entrée
  - Alt+Tiret
  - Alt+F4
  - ImprÉcr
  - Alt+ImprÉcr
  - F1
  - Pause
  - Tabulation
  - Ctrl+Entrée
  - Syst
  - Alt+Syst

- Format d'image : la taille de l'image vidéo de la console virtuelle HTML5 s'adapte automatiquement pour rendre l'image visible. Les options de configuration suivantes s'affichent sous forme de liste déroulante :
  - Maintenance
  - Pas de maintenance

  Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres sélectionnés sur le serveur.
- Mode tactile : la console virtuelle HTML5 prend en charge la fonction Mode tactile. Les options de configuration suivantes s'affichent sous forme de liste déroulante :
  - Direct
  - Relatif

  Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres sélectionnés sur le serveur.
- Accélération de la souris : sélectionnez l'accélération de la souris en fonction du système d'exploitation. Les options de configuration suivantes s'affichent sous forme de liste déroulante :
  - Absolue (Windows, dernières versions de Linux, Mac OS-X)
  - Relative, pas d'accélération
  - Relative (RHEL, versions précédentes de Linux)
  - Linux RHEL 6.x et SUSE Linux Enterprise Server 11 ou version ultérieure

  Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres sélectionnés sur le serveur.
- Média virtuel : cliquez sur l'option **Connect Virtual Media (Connecter un média virtuel)** pour démarrer la session du média virtuel. Le menu du média virtuel affiche l' option **Browse (Parcourir)** qui permet de parcourir et mapper les fichiers IMG et ISO.

REMARQUE : Vous ne pouvez pas mapper des supports physiques tels que les lecteurs USB, les CD ou les DVD à l'aide de la console virtuelle HTML5.

Navigateurs pris en charge

La console virtuelle HTML5 est prise en charge sur les navigateurs suivants :

- Internet Explorer 11
- Chrome 36

Pour en savoir plus sur les navigateurs et les versions pris en charge, consultez les *Notes de mise à jour du contrôleur iDRAC*, disponibles sur **dell.com/idracmanuals**.

Synchronisation des pointeurs de souris

Lorsque vous vous connectez à un système géré via la console virtuelle, la vitesse d'accélération de la souris sur le système géré peut ne pas se synchroniser avec le pointeur de la souris sur la station de gestion et deux pointeurs de souris s'affichent dans le Visualiseur.

Lorsque vous utilisez Red Hat Enterprise Linux ou Novell SUSE Linux, configurez le mode de la souris pour Linux avant de lancer le Visualiseur de console virtuelle. Les paramètres par défaut de la souris du système d'exploitation servent à contrôler la flèche de la souris dans le Visualiseur de console virtuelle.

Lorsque deux curseurs de souris apparaissent dans le visualiseur de la console virtuelle, cela signifie que le système d'exploitation du serveur prend en charge le positionnement relatif. Ceci est typique pour les systèmes d'exploitation Linux ou pour Lifecycle Controller - deux curseurs apparaissent si les paramètres d'accélération des souris du serveur sont différents des paramètres d'accélération des souris du client de la console virtuelle. Pour résoudre ce problème, passez à un curseur unique ou faites correspondre les paramètres d'accélération des souris du système géré et de la station de gestion :

- Pour passer à un curseur unique, sélectionnez **Curseur unique** dans le menu **Outils**.
- Pour définir les paramètres d'accélération des souris , rendez-vous sous **Outils** > **Options de session** > **Souris**. Sous l'onglet **Accélération de souris**, sélectionnez **Windows** ou **Linux**, en fonction du système d'exploitation.

Pour quitter le mode Curseur unique, appuyez sur la touche <F9> ou sur la clé d'arrêt configurée.

REMARQUE : Ceci ne s'applique pas aux systèmes gérés qui exécutent le système d'exploitation Windows, car ils prennent en charge le positionnement absolu.

Lorsque vous utilisez la console virtuelle pour vous connecter à un système géré disposant d'un système d'exploitation Linux récent, des problèmes de synchronisation de souris peuvent apparaître. Ils sont provoqués par la fonction d'accélération de pointeur prévisible du bureau GNOME. Pour corriger la synchronisation de la souris dans la console virtuelle d'iDRAC, désactivez cette fonction. Pour ce faire, dans la section de la souris du fichier **/etc/X11/xorg.conf**, ajoutez :

`Option "AccelerationScheme" "lightweight"`.

Si les problèmes de synchronisation persistent, effectuez les modifications supplémentaires suivantes dans le fichier **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** :

Remplacez les valeurs de `motion_threshold` et de `motion_acceleration` par `-1`.

Si vous désactivez l'accélération de la souris dans le bureau GNOME, dans le Visualiseur de console virtuelle, accédez à **Outils** > **Options de session** > **Souris**. Dans l'onglet **Accélération de la souris**, sélectionnez **Aucune**.

Pour un accès exclusif à la console du serveur géré, vous devez désactiver la console locale et reconfigurer les **Sessions max.** sur la valeur `1` dans la page **Console Virtuelle**.

Envoi de toutes les frappes de touches via la console virtuelle pour le plug-in Java ou ActiveX

Vous pouvez activer l'option **Envoyer toutes les frappes au serveur** et envoyer toutes les frappes et combinaisons de touches depuis la station de gestion au système géré via le visualiseur de la console virtuelle. Si cette option est désactivée, les combinaisons de touches sont redirigées vers la station de gestion sur laquelle la session de la console virtuelle s'exécute. Pour envoyer toutes les touches au serveur, dans le visualiseur de la console virtuelle, allez sous l'onglet **Outils** > **Options de session** > **Général** et sélectionnez l'option **Envoyer toutes les frappes au serveur** pour envoyer les frappes de la station de gestion au système géré.

Le comportement de la fonction Envoyer toutes les frappes au serveur dépend :

- du type de plug-in (Java ou ActiveX) en fonction duquel la session de console virtuelle est lancée ;

  Pour le client Java, la bibliothèque native doit être chargée pour que l'option Envoyer toutes les frappes au serveur et le mode Curseur unique fonctionnent. Si les bibliothèques natives ne sont pas chargées, les options **Envoyer toutes les frappes au serveur** et **Curseur unique** sont désélectionnées. Si vous tentez de sélectionner l'une de ces options, un message d'erreur s'affiche indiquant que les options sélectionnées ne sont pas prises en charge.

  Pour le client ActiveX, la bibliothèque doit être chargée pour que la fonction Envoyer toutes les frappes au serveur fonctionne. Si les bibliothèques natives ne sont pas chargées, l'option **Envoyer toutes les frappes au serveur** est désélectionnée. Si vous tentez de sélectionner cette option, un message d'erreur s'affiche indiquant que la fonction n'est pas prise en charge.

  Pour les systèmes d'exploitation MAC, activez l'option **Activer l'accès pour les périphériques d'aide** dans **Accès universel** pour que la fonction Envoyer toutes les frappes au serveur fonctionne.

- Système d'exploitation s'exécutant sur la station de gestion et le système géré. Les combinaisons de touches significatives pour le système d'exploitation de la station de gestion ne sont pas envoyées au système géré ;
- Mode du Visualiseur de console virtuelle ; Avec fenêtres ou Plein écran.

  En mode Plein écran, l'option **Envoyer toutes les frappes au serveur** est activée par défaut.

  En mode Avec fenêtres, les touches sont envoyées uniquement lorsque le Visualiseur de console virtuelle est visible et actif.

  Lorsque vous passez du mode Plein écran au mode Avec fenêtres, l'état précédent de l'envoi de toutes les touches est réactivé.

Concepts associés

Session de console virtuelle Java-sur le système d'exploitation Windows , page 244
Session de console virtuelle Java exécutée sur le système d'exploitation Linux , page 245
Session de console virtuelle ActiveX sur le système d'exploitation Windows , page 246

Session de console virtuelle Java-sur le système d'exploitation Windows

- La touche Ctrl+Alt+Suppr n'est pas envoyée au système géré, mais elle est toujours interprétée par la station de gestion.
- Lorsque l'envoi de toutes les frappes au serveur est activé, les touches suivantes ne sont pas envoyées au système géré :
  - Touche Précédent du navigateur
  - Touche Suivant du navigateur
  - Touche Actualiser du navigateur
  - Touche Arrêt du navigateur
  - Touche de recherche du navigateur
  - Touche Favoris du navigateur
  - Touche de démarrage et Origine du navigateur
  - Touche de coupure du son

- Touche de diminution du volume
- Touche d'augmentation du volume
- Touche Piste suivante
- Touche Piste précédente
- Touche Arrêt média
- Touche Lecture/Pause
- Touche Démarrage de la messagerie
- Touche Sélection de média
- Touche Application 1
- Touche Application 2

- Toutes les touches individuelles (non pas une combinaison de touches, mais une seule frappe de touche) sont toujours envoyées au système géré. Ceci inclut toutes les touches de fonction, les touches Maj, Alt, Ctrl et les touches Menu. Certaines de ces touches affectent la station de gestion et le système géré.

  Par exemple, si la station de gestion et le système géré utilisent le système d'exploitation Windows et que l'envoi de toutes les touches est désactivé, lorsque vous appuyez sur la touche Windows pour ouvrir le menu **Démarrer**, le menu **Démarrer** s'ouvre sur la station de gestion et le système géré. Cependant, si l'envoi de toutes les touches est activé, le menu **Démarrer** s'ouvre sur le système géré, mais pas sur la station de gestion.

- Lorsque l'envoi de toutes les touches est désactivé, le comportement dépend des combinaisons de touches utilisées et des combinaisons spéciales interprétées par le système d'exploitation sur la station de gestion.

Session de console virtuelle Java exécutée sur le système d'exploitation Linux

Le comportement mentionné pour le système d'exploitation Windows s'applique également au système d'exploitation Linux avec les exceptions suivantes :

- Lorsque l'envoi de toutes les frappes au serveur est activé, <Ctrl+Alt+Suppr> est envoyé au système d'exploitation du système géré.
- Les touches Magic SysRq sont des combinaisons de touches interprétées par Linux Kernel. Elles sont utiles si le système d'exploitation du système géré de la station de gestion ou du système géré se bloque et que vous devez récupérer le système. Vous pouvez activer les touches magiques SysRq sur le système d'exploitation Linux en utilisant les méthodes suivantes :
  - Ajoutez une entrée à **/etc/sysctl.conf**
  - echo 1 > /proc/sys/kernel/sysrq
- Lorsque l'envoi de toutes les touches au serveur est activé, les touches magiques SysRq sont envoyées au système d'exploitation du système géré. Le comportement de la séquence de touches pour réinitialiser le système, à savoir redémarrer sans démontage ou synchronisation, varie selon que SysRq est activé ou désactivé sur la station de gestion :
  - Si SysRq et activé sur la station de gestion, <Ctrl+Alt+SysRq+b> ou <Alt+SysRq+b> réinitialise la station de gestion, quel que soit l'état du système.
  - Si SysRq est désactivé, les touches <Ctrl+Alt+SysRq+b> ou <Alt+SysRq+b> réinitialisent le système d'exploitation du système géré.
  - Les autres combinaisons de touches SysRq (telles que, <Alt+SysRq+k>, <Ctrl+Alt+SysRq+m>, etc.) sont envoyées au système géré, que les touches SysRq soient activées ou non sur la station de gestion.

Utilisation des touches magiques SysRq via la console distante

Vous pouvez activer les touches magiques SysRq via la console distante à l'aide de l'une des méthodes suivantes :

- outil IPMI Opensource
- À l'aide de SSH/Telnet ou du Connecteur série externe

Utilisation de l'outil IPMI opensource

Assurez-vous que les paramètres du BIOS/iDRAC prennent en charge la redirection de console à l'aide des communications SOL.

1. À l'invite de commande, exécutez la commande SOL activate :

   ```
   Ipmitool -I lanplus -H <ipaddr> -U <username> -P <passwd> sol activate
   ```

   La session SOL est activée.
2. Une fois que le serveur démarre à partir du système d'exploitation, l'invite de connexion`localhost.localdomain` s'affiche. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de votre système d'exploitation.
3. Si SysRq n'est pas activé, activez-le en utilisant `echo 1 >/proc/sys/kernel/sysrq`.

4. Exécutez la séquence d'interruption `~ B`.
5. Utilisez la touche magique SysRq pour activer la fonction SysRq. Par exemple, la commande suivante affiche les informations de mémoire sur la console :

```
echo m > /proc/sysrq-trigger displays
```

À l'aide de SSH ou Telnet ou d'un connecteur série externe - directement connecté via le câble série

1. Pour les sessions Telnet/SSH, après vous être connecté à l'aide du nom d'utilisateur et du mot de passe iDRAC, à l'invite `/admin>`, exécutez la commande `console com2`. L'invite `localhost.localdomain` s'affiche.
2. Pour la redirection de console à l'aide du connecteur série externe directement connecté au système via un câble série, l'invite `localhost.localdomain` apparaît après le démarrage du serveur à partir du système d'exploitation.
3. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de votre système d'exploitation.
4. Si NDMP n'est pas activé, activez-le avec `echo 1 >/proc/sys/kernel/sysrq`.
5. Utilisez la touche magique pour activer la fonction SysRq. Par exemple, la commande suivante redémarre le serveur :

```
echo b > /proc/sysrq-trigger
```

REMARQUE : Il n'est donc pas nécessaire d'exécuter une séquence d'interruption avant d'utiliser la touche magique SysRq.

Session de console virtuelle ActiveX sur le système d'exploitation Windows

Le comportement de l'envoi de toutes les frappes au serveur dans une session de console virtuelle ActiveX exécutée sur le système d'exploitation Windows est similaire au comportement expliqué pour une session de console virtuelle Java sur la station de gestion, mais avec les exceptions suivantes :

- Lorsque l'envoi de toutes les touches est désactivé et que vous appuyez sur F1, vous affichez l'aide de l'application sur la station de gestion et le système géré et le message suivant s'affiche :

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- Les touches de média peuvent ne pas être bloquées de manière explicite.
- Les combinaisons de touches <Alt + Espace>, <Ctrl + Alt + +>, <Ctrl + Alt + -> ne sont pas envoyées au système géré et elles sont interprétées par le système d'exploitation de la station de gestion.

15

Gestion de Média Virtuel

Média Virtuel permet au serveur géré d'accéder aux périphériques de support sur la station de gestion ou aux images de CD/DVD ISO sur un partage de réseau comme s'il s'agissait de périphériques sur le serveur géré.

Avec la fonction Média Virtuel, vous pouvez :

- Accéder à distance à un support connecté à un système distant sur le réseau
- Installer des applications
- Mettre à jour les pilotes
- Installer un système d'exploitation sur le système géré

Il s'agit d'une fonctionnalité sous licence pour les serveurs rack et tour. Elle est disponible par défaut sur les serveurs lames.

Les principales fonctions sont les suivantes :

- Prise en charge des lecteurs optiques virtuels (CD/DVD), des lecteurs de disquette (y compris les lecteurs USB) et des lecteurs Flash USB.
- Vous pouvez connecter un seul lecteur de disquette ou lecteur Flash USB, une seule image ou clé et un seul lecteur optique à un système géré dans la station de gestion. Les lecteurs de disquette pris en charge incluent une image de disquette ou un lecteur de disquette disponible. Les lecteurs optiques pris en charge incluent un seul lecteur optique maximum disponible ou un seul fichier image ISO.

  REMARQUE : Lorsque la licence iDRAC expire ou est supprimée, la console virtuelle et les ports média virtuel sont automatiquement fermés, entraînant l'arrêt de toutes les sessions de console virtuelle et de média virtuel.

  L'illustration suivante montre une configuration Média Virtuel type.

- Le lecteur de disquette virtuel d'iDRAC n'est pas accessible depuis les machines virtuelles.
- Un média virtuel connecté émule un périphérique physique sur le système géré.
- Sur les système gérés Windows, les lecteurs Média Virtuel sont montés automatiquement s'ils sont connectés et configurés avec une lettre d'unité.
- Sur les systèmes gérés Linux avec certaines configurations, les lecteurs Média Virtuel ne sont pas montés automatiquement. Pour monter les lecteurs manuellement, utilisez la commande mount.
- Toutes les demandes d'accès aux lecteurs virtuels du système géré sont envoyées à la station de gestion dans le réseau.
- Les périphériques virtuels apparaissent comme deux lecteurs sur le système géré sans que le support soit installé dans les lecteurs.
- Vous pouvez partager le lecteur de CD/DVD (lecture seule) de la station de gestion, mais pas un média USB, entre deux systèmes gérés.
- Média Virtuel exige une bande passante réseau disponible d'au moins 128 Kb/s.
- Si un basculement LOM ou NIC se produit, la session Média Virtuel est déconnectée.

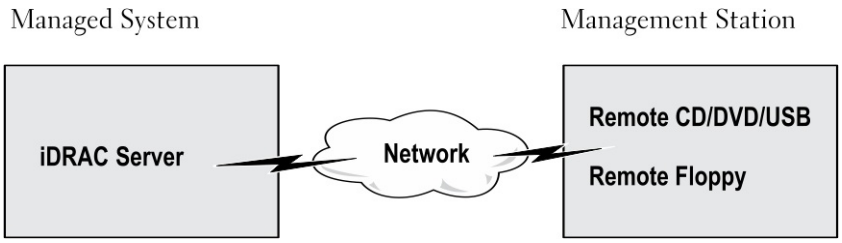


Figure 4. Configuration Média Virtuel

Sujets :

- Lecteur et périphériques pris en charge
- Configuration de média virtuel
- Accès à un média virtuel
- Définition de la séquence de démarrage via le BIOS
- Activation du démarrage unique pour Média Virtuel

Lecteur et périphériques pris en charge

Le tableau suivant répertorie les lecteurs pris en charge via Média Virtuel.

Tableau 40. Lecteur et périphériques pris en charge

Lecteur	Support de stockage compatible
Lecteurs optiques virtuels	• Lecteur de disquette 1,44 hérité avec disquette 1,44 • CD-ROM • DVD • CD-RW • Lecteur avec support CD-RO
Lecteurs de disquette virtuels	• Fichier image de CD-ROM/DVD au format ISO9660 • Fichier image de disquette ISO9660 au format ISO9660
Lecteurs Flash USB	• Lecteur de CD-ROM USB avec support CD-ROM • Fichier image USB au format ISO9660

Configuration de média virtuel

Avant de définir les paramètres Média Virtuel, configurez le navigateur Web pour utiliser le plug-in Java ou ActiveX

Concepts associés

Configuration des navigateurs Web pour utiliser la console virtuelle , page 60

Configuration de média virtuel à l'aide de l'interface Web d'iDRAC

Pour définir les paramètres Média Virtuel :

PRÉCAUTION : Ne réinitialisez pas iDRAC lorsque vous exécutez une session Média Virtuel afin de ne pas obtenir des résultats indésirables, notamment une perte de données.

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Média connecté**.
2. Définissez les paramètres nécessaires. Pour en savoir plus, voir l'*Aide en ligne d'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 en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration de Média Virtuel à l'aide de l'utilitaire de configuration d'iDRAC

Vous pouvez connecter, déconnecter ou connecter automatiquement un média virtuel en utilisant l'utilitaire de configuration d'iDRAC. Pour ce faire :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **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 des besoins.
   Pour plus d'informations sur les options, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   Les paramètres du média virtuel sont configurés.

État de média connecté et réponse du système

Le tableau suivant indique la réponse du système en fonction du paramètre Média connecté.

Tableau 41. 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 permettre une visibilité des lecteurs vides. Pour ce faire, dans l'Explorateur Windows, dans le menu **Organiser**, cliquez sur **Options des dossiers et de recherche**. Sous l'onglet **Afficher**, 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 les navigateurs Web.

Le média virtuel et RFS sont mutuellement exclusifs. Si la connexion RFS est active et que vous tentez de lancer le client média virtuel, le message d'erreur suivant s'affiche : *Le média virtuel est actuellement indisponible. Une session média virtuel ou de partage de fichiers à distance est en cours d'utilisation.*

Si la connexion RFS n'est pas active, et que vous tentez de lancer le client média virtuel, celui-ci est lancé avec succès. Vous pouvez alors utiliser le client média virtuel pour mapper des périphériques et des fichiers aux lecteurs virtuels du média virtuel.

Concepts associés

Configuration des navigateurs Web pour utiliser la console virtuelle , page 60
Configuration de média virtuel , page 248

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 iDRAC, accédez à **Présentation** > **Serveur** > **Console virtuelle**.
   La page **Console virtuelle** s'affiche.
2. Cliquez sur **Lancer Console virtuelle**.
   Le **Visualiseur de console virtuelle** s'ouvre.
   REMARQUE : Sous Linux, Java est le type de plug-in par défaut pour accéder à la console virtuelle. Sous Windows, ouvrez le fichier `.jnlp` pour lancer la console virtuelle à l'aide de Java.
3. Cliquez sur **Média Virtuel** > **Lancer Média Virtuel**.
   La session de média virtuel est établie et le menu **Média virtuel** affiche la liste des périphériques disponibles en vue du mappage.
   REMARQUE : La fenêtre du **Visualiseur de console virtuelle** doit rester active pendant que vous accédez à Média Virtuel.

Concepts associés

Configuration des navigateurs Web pour utiliser la console virtuelle , page 60
Configuration de média virtuel , page 248
Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX , page 241

Lancement de Média Virtuel sans utiliser la console virtuelle

Avant de lancer Média Virtuel lorsque la **Console virtuelle** est désactivée, vérifiez que :

- Média Virtuel est *connecté*.
- Le système est configuré pour afficher les lecteurs vides. Pour ce faire, dans l'Explorateur Windows, accédez à **Options de dossier**, désélectionnez l'option **Masquer les lecteurs vides dans le dossier Ordinateur**, puis cliquez sur **OK**.

Pour lancer Média Virtuel lorsque la console virtuelle est désactivée :

1. Dans l'interface Web d'iDRAC, allez à **Présentation** > **Serveur** > **Console virtuelle**.
   La page **Console virtuelle** s'affiche.
2. Cliquez sur **Lancer Console virtuelle**.
   Le message suivant s'affiche :

   ```
   Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
   ```

3. Cliquez sur **OK**.
   La fenêtre **Média virtuel** s'affiche.
4. Dans le menu **Média virtuel** , cliquez sur **Mappage du CD/DVD** ou **Mappage de disque amovible**.
   Pour plus d'informations, voir Mappage de lecteur virtuel.

   REMARQUE : Les lettres de lecteur de périphérique virtuel sur le système géré ne coïncident pas avec les lettres de lecteur physique sur la station de gestion.

   REMARQUE : Le Média Virtuel peut ne pas fonctionner correctement sur les clients du système d'exploitation Windows configurés avec la sécurité renforcée d'Internet Explorer. Pour résoudre le problème, voir la documentation du système d'exploitation ou contacter l'administrateur système.

   REMARQUE : Le plug-in HTML5 n'est pas pris en charge pour les médias virtuels autonomes.

Concepts associés

Configuration de média virtuel , page 248
Désactivation des messages d'avertissement tout en lançant la console virtuelle ou le média virtuel via le plug-in Java ou ActiveX , page 241

Ajout d'images Média Virtuel

Vous pouvez créer une image média du dossier à distance et la monter en tant que périphérique USB connecté sur le système d'exploitation du serveur. Pour ajouter des images de média virtuel :

1. Cliquez sur **Média virtuel** > **Créer une image...**.
2. Dans le champ **Dossier source**, cliquez sur **Parcourir** et naviguez vers le dossier ou le répertoire à utiliser comme source du fichier image. Le fichier image se trouve sur la station de gestion ou sur le lecteur C: du système géré.
3. Dans le champ **Nom du fichier d'image**, le chemin d'accès par défaut au stockage des fichiers d'image créés (en règle générale, le répertoire du bureau) apparaît. Pour changer cet emplacement, cliquez sur **Parcourir** et recherchez un emplacement.
4. Cliquez sur **Créer une image**.

   Le processus de création d'image démarre. Si l'emplacement du fichier d'image se trouve au sein du dossier source, le message d'avertissement qui s'affiche indique que la création d'image ne peut pas se poursuivre car l'emplacement du fichier d'image au sein du dossier source crée une boucle à l'infini. Si l'emplacement du fichier d'image ne se trouve pas au sein du dossier source, la création de l'image se poursuit.

   Une fois l'image créée, un message indiquant que la création a réussi s'affiche.
5. Cliquez sur **Terminer**.

L'image est créée.

Lorsque le dossier est ajouté comme image, un fichier **.img** est créé sur le bureau de la station de gestion d'où la fonction est utilisée. Si ce fichier **.img** est déplacé ou supprimé, l'entrée correspondante du dossier dans le menu **Média Virtuel** ne fonctionne pas. Par conséquent, il est recommandé de ne pas déplacer ni de supprimer le fichier **.img** lorsque l'*image* est en cours d'utilisation. Toutefois, le fichier **.img** peut être supprimé après désélection de l'entrée appropriée et en utilisant la commande de **suppression d'image** pour supprimer l'entrée.

Affichage des informations détaillées d'un périphérique virtuel

Pour afficher les détails du périphérique virtuel, dans le visualiseur de console virtuelle, cliquez sur **Outils** > **Statistiques**. Dans la fenêtre **Statistiques** , la section **Média virtuel** affiche les périphériques virtuels mappés et l'activité de lecture/écriture correspondant à chaque périphérique. Si le média virtuel est connecté, ces informations s'affichent. Si le média virtuel n'est pas connecté, le message « Média virtuel non connecté » s'affiche.

Si le média virtuel est lancé sans l'aide de la console virtuelle, la section **Média virtuel** apparaît sous forme de boîte de dialogue. Elle fournit des informations sur les périphériques mappés.

Réinitialisation USB

Pour réinitialiser le périphérique USB :

1. Dans le visualiseur de console virtuelle, cliquez sur **Outils** > **Statistiques**.
   La fenêtre de **Statistiques** s'affiche.
2. Dans la section **Média virtuel**, cliquez sur **Réinitialisation USB**.
   Un message affiche un avertissement à l'attention de l'utilisateur pour lui indiquer que la réinitialisation de la connexion USB peut affecter toutes les entrées vers le périphérique cible, y compris Média Virtuel, le clavier et la souris.
3. Cliquez sur **Oui**.
   L'USB est réinitialisé.

   REMARQUE : Média Virtuel 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 : Pour utiliser Média Virtuel ActiveX, vous devez disposer des privilèges administratifs permettant de mapper un DVD ou un lecteur Flash USB de système d'exploitation (connecté à la station de gestion). Pour mapper les lecteurs, lancez IE en tant qu'administrateur ou ajoutez l'adresse IP d'iDRAC à la liste des sites de confiance.

1. Pour établir une session de média virtuel, à partir du menu **Média virtuel**, cliquez sur **Connecter le média virtuel**.
   Pour chaque périphérique disponible pour mappage depuis le serveur hôte, un élément de menu apparaît sous le menu **Média virtuel**. Cet élément porte le nom du type de périphérique, par exemple :
   - Mapper CD/DVD
   - Mapper le disque amovible
   - Mapper une disquette

   REMARQUE : L'élément de menu **Mappage du lecteur de disquette** apparaît dans la liste si l'option **Émulation de disquette** est activée sur la page de **média connecté**. Quand **Émulation de disquette** est activée, **Mappage du disque amovible** est remplacé par **Mappage du lecteur de disquette**.

   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.

   REMARQUE : Vous ne pouvez pas mapper des supports physiques tels que les lecteurs USB, les CD ou les DVD à l'aide de la console virtuelle basée sur HTML5.

2. Cliquez sur le type de périphérique que vous souhaitez mapper.

   REMARQUE : La session active indique si une session de média virtuel est actuellement active à partir de la session d'interface Web actuelle, à partir d'une autre session d'interface Web ou à partir de VMCLI.

3. Dans le champ **Lecteur/Fichier d'image**, sélectionnez le périphérique dans la liste déroulante.

   La liste contient tous les périphériques disponibles (non mappés) que vous pouvez mapper (CD/DVD, Disque amovible, Lecteur de disquette) et les types de fichier d'image que vous pouvez mapper (ISO ou IMG). Les fichiers d'image se trouvent dans le répertoire de fichiers d'image par défaut (en règle générale, le bureau de l'utilisateur). Si le périphérique n'est pas disponible dans la liste déroulante, cliquez sur **Parcourir** pour le spécifier.

   Le bon type de fichier pour CD/DVD est ISO, et IMG pour disquette et disque amovible.

   Lorsque l'image est créée dans le chemin par défaut (ordinateur de bureau), lorsque vous sélectionnez **Mappage de disque amovible**, l'image créée est disponible pour être sélectionnée dans le menu déroulant.

   Si l'image est créée dans un autre emplacement, lorsque vous sélectionnez **Mappage de disques amovibles**, l'image créée n'est pas disponible dans le menu déroulant. Cliquez sur **Parcourir** pour spécifier l'image.

4. Sélectionnez **lecture seule** pour mapper les périphériques enregistrables en lecture seule.

   Pour les périphériques CD/DVD, cette option est activée par défaut et vous ne pouvez pas la désactiver.

   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 mappé, le nom de son élément de menu **Média virtuel** change pour refléter le nom du périphérique. Par exemple, si le périphérique CD/DVD est mappé sur un fichier image nommé `foo.iso`, l'élément du menu CD/DVD du menu Média virtuel se nomme **foo.iso mappé sur le CD/DVD**. Une coche en regard de cet élément de menu indique qu'il est mappé.

Concepts associés

Affichage des lecteurs virtuels corrects pour le mappage , page 252
Ajout d'images Média Virtuel , page 250

Affichage des lecteurs virtuels corrects pour le mappage

Sur une station de gestion Linux, la fenêtre du **Client** de Média Virtuel peut contenir des lecteurs de disque et de disquette qui ne font pas partie de la station de gestion. Pour que les lecteurs virtuels corrects soient disponibles pour l'adressage, vous devez activer la configuration de port du disque dur SATA connecté. Pour ce faire :

1. Redémarrez le système d'exploitation sur la station de gestion. Au cours du POST, appuyez sur <F2> pour entrer dans le programme de **Configuration du système**.
2. Accédez à **Paramètres SATA**. Les informations de port s'affichent.
3. Activez les ports présents et connectés au disque dur.
4. Accédez à la fenêtre du **Client** de Média Virtuel. Elle contient les lecteurs corrects qui peuvent être mappés.

Concepts associés

Mappage d'un lecteur virtuel , page 251

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**.

   Un message s'affiche vous demandant de confirmer.
2. Cliquez sur **Oui**.
   La case à cocher correspondant à cet élément de menu ne s'affiche pas, ce qui signifie qu'il n'existe aucun mappage sur le serveur hôte.

   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, le volume non mappé peut ne pas être disponible sur le client. Redémarrez le système ou montez le périphérique manuellement sur le système client pour afficher le périphérique.

Définition de la séquence de démarrage via le BIOS

En utilisant l'utilitaire System BIOS Settings, vous pouvez configurer le système géré pour qu'il démarre depuis les lecteurs optiques virtuels ou les lecteurs de disquette virtuels.

REMARQUE : Le changement de Média Virtuel en cours de connexion peut interrompre la séquence de démarrage du système.

Pour permettre au système géré de démarrer :

1. Démarrez le système géré.
2. Appuyez sur <F2> pour accéder à la page **Configuration du système**.
3. Accédez à **Paramètres du BIOS du système** > **Paramètres de démarrage** > **Paramètres de démarrage du BIOS** > **Séquence de démarrage**.
   Dans la fenêtre contextuelle, les lecteurs optiques virtuels et les lecteurs de disquette virtuels sont répertoriés avec les périphériques de démarrage standard.
4. Vérifiez que le lecteur virtuel est activé et qu'il est le premier périphérique avec un support amorçable. Si nécessaire, suivez les instructions qui s'affichent pour modifier la séquence de démarrage.
5. Cliquez sur **OK**, revenez à la page **Paramètres BIOS du système** et cliquez sur **Terminer**.
6. Cliquez sur **Oui** pour enregistrer les modifications et quitter.

   Le système géré redémarre.

   Il tente de démarrer depuis un périphérique amorçable en fonction de la séquence de démarrage. Si le périphérique virtuel est connecté et qu'un support amorçable est présent, le système démarre depuis le périphérique virtuel. Dans le cas contraire, il ignore le périphérique comme dans le cas d'un périphérique physique ne contenant pas de support amorçable.

Activation du démarrage unique pour Média Virtuel

Vous pouvez changer la séquence de démarrage uniquement une fois lorsque vous démarrez le système après avoir connecté un périphérique Média Virtuel distant.

Avant d'activer l'option de démarrage unique :

- Vérifiez que vous disposez du privilège de *configuration d'utilisateur*.
- Associez les lecteurs locaux ou virtuels (CD/DVD, lecteur de disquette ou lecteur Flash USB) au média ou à l'image amorçable en utilisant les options Média Virtuel.
- Média Virtuel est *connecté* pour que les lecteurs virtuels apparaissent dans la séquence de démarrage.

Pour activer l'option de démarrage unique et démarrer le système géré depuis Média Virtuel :

1. Dans l'interface Web 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.

Concepts associés

Mappage d'un lecteur virtuel , page 251
Configuration de média virtuel , page 248

16

Installation et utilisation de l'utilitaire VMCLI

L'utilitaire WMCLI (Virtual Media Command Line Interface) est une interface qui fournit des fonctions de média virtuel de la station de gestion vers iDRAC sur le système géré. Utilisez cet utilitaire pour accéder aux fonctions de média virtuel, notamment aux fichiers images et aux disques physiques, pour déployer un système d'exploitation sur plusieurs systèmes distants dans un réseau.

REMARQUE : VMCLI ne prend en charge que le protocole de sécurité TLS 1.0.

L'utilitaire VMCLI prend en charge les fonctionnalités suivantes :

- Gestion des périphériques amovibles ou des images accessibles via Média Virtuel.
- Fin de la session lorsque l'option **Démarrage unique** du micrologiciel iDRAC est activée.
- Sécurisation des communications vers iDRAC à l'aide du protocole SSL (Secure Sockets Layer)
- Exécutez les commandes VMCLI jusqu'à ce que :
  - Les connexions se terminent automatiquement.
  - Un système d'exploitation termine le processus.

REMARQUE : Pour mettre fin au processus dans Windows, utilisez le Gestionnaire des tâches.

Sujets :

- Installation de VMCLI
- Exécution de l'utilitaire VMCLI
- Syntaxe VMCLI

Installation de VMCLI

L'utilitaire VMCLI est inclus dans le DVD *Dell Systems Management Tools and Documentation*.

Pour installer l'utilitaire VMCLI :

1. Insérez le DVD *Dell Systems Management Tools and Documentation* dans le lecteur de DVD.
2. Suivez les instructions qui s'affichent pour installer les outils DRAC.
3. Après l'installation, vérifiez le dossier **install\Dell\SysMgt\rac5** pour vous assurer que **vmcli.exe** existe. De même, vérifiez le chemin pour UNIX.
   L'utilitaire VMCLI est installé sur le système.

Exécution de l'utilitaire VMCLI

- Si le système d'exploitation nécessite des privilèges spécifiques ou d'appartenir à un groupe, vous devez disposer de privilèges similaires pour pouvoir exécuter des commandes VMCLI.
- Sur les systèmes Windows, les utilisateurs non-administrateurs doivent avoir les privilèges **Utilisateur avec pouvoir** pour pouvoir exécuter l'utilitaire VMCLI.
- Sur les systèmes Linux, pour accéder à iDRAC et exécuter l'utilitaire VMCLI et journaliser les commandes utilisateur, les utilisateurs non-administrateurs doivent utiliser `sudo` comme préfixe dans les commandes VMCLI. Toutefois, pour ajouter ou modifier des utilisateurs dans le groupe Administrateurs VMCLI, utilisez la commande `visudo`.

Syntaxe VMCLI

L'interface VMCLI est identique sur les systèmes Windows et Linux. La syntaxe VMCLI est la suivante :

```
VMCLI [parameter] [operating_system_shell_options]
```

Par exemple, `vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

Le *paramètre* permet à VMCLI de se connecter au serveur défini, d'accéder à iDRAC et de s'adresser au support virtuel spécifié.

REMARQUE : La syntaxe VMCLI tient compte de la casse.

À des fins de sécurité, il est recommandé d'utiliser les paramètres VMCLI suivants :

- `vmcli -i` : permet d'utiliser une méthode interactive pour démarrer VMCLI. Elle permet de masquer le nom d'utilisateur et le mot de passe lorsque les processus sont examinés par d'autres utilisateurs.
- vmcli `-r <iDRAC-IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {< device-name > | < image-file >}` : indique si le certificat CA iDRAC est valide. Si le certificat n'est pas valide, un message d'avertissement s'affiche lorsque vous exécutez la commande. Cependant, la commande aboutit et une session VMCLI est établie. Pour plus d'informations sur les paramètres VMCLI, voir l'*Aide VMCLI* ou les *Pages Man VMCLI*.

Concepts associés

Commandes VMCLI pour accéder à Média Virtuel , page 255
Options shell de système d'exploitation WMCLI , page 255

Commandes VMCLI pour accéder à Média Virtuel

Le tableau suivant répertorie les commandes VMCLI nécessaires pour accéder à un média virtuel différent.

Tableau 42. Commandes VMCLI

Média virtuel	Commande
Lecteur de disquette	`vmcli -r [RAC IP or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]`
Disquette amorçable ou image de clé USB	`vmcli -r [iDRAC IP address] [iDRAC user name]` `-p [iDRAC password] -f [floppy.img]`

Lecteur de CD en utilisant l'option -f	`vmcli -r [iDRAC IP address] -u [iDRAC user name]`
	`-p [iDRAC password] -f [device name]|[image file]-f [cdrom - dev`
	`]`

Image CD/DVD amorçable	`vmcli -r [iDRAC IP address] -u [iDRAC user name]` `-p [iDRAC password] -c [DVD.img]`

Si le fichier n'est pas protégé contre l'écriture, Média virtuel peut écrire sur le fichier image. Pour que Média Virtuel n'écrive pas sur le support :

- Configurez le système d'exploitation pour protéger contre l'écriture un fichier image de disquette qui ne doit pas être remplacé.
- Utilisez la fonction de protection contre l'écriture du périphérique.

Lors de la virtualisation des fichiers images en lecture seule, plusieurs sessions peuvent utiliser simultanément le même support d'image.

Lors de la virtualisation des lecteurs physiques, une seule session peut accéder à un lecteur physique donné à la fois.

Options shell de système d'exploitation WMCLI

VMCLI utilise des options d'environnement pour activer les fonctions suivantes de système d'exploitation :

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

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

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

- Exécution en arrière-plan : par défaut, l'utilitaire VMCLI s'exécute au premier plan. Utilisez les fonctions d'environnement de commande du système d'exploitation pour exécuter l'utilitaire en arrière-plan.

  Par exemple, dans un système d'exploitation Linux, le caractère perluète (&) suivant la commande fait que le programme est créé comme un nouveau processus en arrière-plan. Cette technique est utile dans les programmes de scripts, car elle permet au script de continuer après le démarrage d'un nouveau processus pour la commande VMCLI (sinon le script se bloque jusqu'à la fin du programme VMCLI).

  Lorsque plusieurs sessions VMCLI démarrent, utilisez les fonctions du système d'exploitation pour lister et mettre fin aux processus.

17

Gestion de la carte SD vFlash

La carte SD vFlash est une carte Secure Digital (SD) qui se connecte dans le logement de carte SD vFlash du système. Vous pouvez utiliser une carte de 16 Go maximum. Après avoir inséré la carte, vous devez activer la fonctionnalité vFlash pour créer et gérer des partitions. vFlash est une fonction sous licence.

Si la carte n'est pas disponible dans le logement de carte SD vFlash du système, le message d'erreur suivant s'affiche dans l'interface web d'iDRAC dans **Présentation** > **Serveur** > **vFlash** :

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

REMARQUE : Veillez à insérer uniquement une carte SD compatible vFlash dans le logement de carte SD iDRAC. Si vous insérez une carte non compatible, le message d'erreur suivant s'affiche lorsque vous initialisez la carte : *Erreur lors de l'initialisation de la carte SD.*

Les principales fonctions sont les suivantes :

- Fourniture d'un espace de stockage et émulation de périphériques USB.
- Création de 16 partitions maximum. Ces partitions, lorsqu'elles sont connectées au système, sont présentées comme lecteur de disquette, disque dur ou lecteur CD/DVD en fonction du mode d'émulation sélectionné.
- Création de partitions depuis les types de systèmes de fichiers compatibles. Prise en charge du format **.img** pour disquette, du format **.iso** pour CD/DVD et des formats **.iso** et **.img** pour les types d'émulation de disque dur.
- Création de périphériques USB amorçables.
- Démarrage uniquement depuis un périphérique USB émulé.

  REMARQUE : Il peut arriver qu'une licence vFlash expire pendant une opération vFlash. Dans ce cas, l'opération en cours vFlash se termine normalement.

REMARQUE : Si le mode FIPS est activé, vous ne pouvez pas effectuer d'actions vFlash.

Sujets :

- Configuration d'une carte SD vFlash
- Gestion des partitions vFlash

Configuration d'une carte SD vFlash

Avant de configurer vFlash, assurez-vous que la carte SD vFlash est installée sur le système. Pour plus d'informations sur l'installation et le retrait de la carte sur le système, voir le *Hardware Owner's Manual* (Manuel du propriétaire du matériel) du système sur le site **dell.com/support/manuals**.

REMARQUE : Vous devez disposer du privilège d'Accès au média virtuel pour pouvoir activer ou désactiver vFlash et initialiser la carte.

Concepts associés

Affichage des propriétés d'une carte SD vFlash , page 257
Activation ou désactivation de la fonctionnalité vFlash , page 258
Initialisation d'une carte SD vFlash , page 259

Affichage des propriétés d'une carte SD vFlash

Après avoir activé la fonctionnalité vFlash, vous pouvez afficher les propriétés d'une carte SD à l'aide de l'interface Web iDRAC ou RACADM.

Affichage des propriétés d'une carte SD vFlash à l'aide de l'interface Web

Pour afficher les propriétés d'une carte SD vFlash, dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **vFlash**. La page **Propriétés de la carte SD** s'affiche. Pour en savoir plus sur les propriétés affichées, voir l'*Aide en ligne d'iDRAC*.

Affichage des propriétés d'une carte SD vFlash à l'aide de RACADM

Pour afficher les propriétés d'une carte SD vFlash à l'aide de RACADM, utilisez la commande `get` avec les objets suivants :

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

Pour plus d'informations sur ces objets, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Affichage des propriétés d'une carte SD vFlash à l'aide de l'utilitaire de configuration d'iDRAC

Pour afficher les propriétés d'une carte SD vFlash, dans l'**Utilitaire de Configuration d'iDRAC**, accédez à **Paramètres du support et du port USB**. La page **Paramètres du support et du port USB** affiche les propriétés. Pour en savoir plus sur les propriétés affichées, voir l'*Aide en ligne de l'utilitaire de Configuration d'iDRAC*.

Activation ou désactivation de la fonctionnalité vFlash

Vous devez activer la fonctionnalité vFlash pour pouvoir gérer les partitions.

Activation ou désactivation de la fonctionnalité vFlash à l'aide de l'interface Web

Pour activer ou désactiver la fonctionnalité vFlash :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash**.
   La page **Propriétés de la carte SD** s'affiche.
2. Sélectionnez ou désélectionnez l'option **vFLASH activé** pour activer ou désactiver la fonctionnalité vFlash. Si une partition vFlash est connectée, vous ne pouvez pas désactiver vFlash et un message d'erreur s'affiche.

   REMARQUE : Si la fonctionnalité vFlash est désactivée, les propriétés de la carte SD ne s'affichent pas.

3. Cliquez sur **Appliquer**. La fonctionnalité vFlash est activée ou désactivée en fonction de la sélection.

Activation ou désactivation de la fonctionnalité vFlash à l'aide de RACADM

Pour activer ou désactiver la fonctionnalité vFlash à l'aide de l'interface RACADM :

```
racadm set iDRAC.vflashsd.Enable [n]
```

n=0

Disabled (désactivé)

n=1

Activée

REMARQUE : La commande RACADM fonctionne uniquement si une carte SD est présente. Dans le cas contraire, le message suivant s'affiche : *ERREUR : carte SD absente*.

Activation ou désactivation de la fonctionnalité vFlash à l'aide de l'utilitaire de configuration d'iDRAC

Pour activer ou désactiver la fonctionnalité vFlash :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Paramètres de port USB et média**.
   La page **Paramètres d'iDRAC. Paramètres de port USB et de média** s'affiche.
2. Dans la section **Média vFlash**, sélectionnez **Activé** pour activer la fonctionnalité vFlash ou **Désactivé** pour la désactiver.
3. Cliquez successivement sur **Retour**, **Terminer** et **Oui**.
   La fonctionnalité vFlash est activée ou désactivée en fonction de la sélection.

Initialisation d'une carte SD vFlash

L'initialisation reformate la carte SD et configure les informations système vFlash sur la carte.

REMARQUE : Si la carte SD est protégée en écriture, l'option Initialiser est désactivée.

Initialisation d'une carte SD vFlash à l'aide de l'interface Web

Pour initialiser une carte vFlash SD :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash**.
   La page **Propriétés de la carte SD** s'affiche.
2. Activez **vFLASH** et cliquez sur **Initialiser**.

   Tout le contenu existant est supprimé et la carte est reformatée avec les nouvelles informations système vFlash.

   Si une partition vFlash est connectée, l'opération d'initialisation échoue et un message d'erreur s'affiche.

Initialisation d'une carte SD vFlash à l'aide de RACADM

Pour initialiser une carte SD vFlash à l'aide de l'interface RACADM :

```
racadm set iDRAC.vflashsd.Initialized 1
```

Toutes les partitions existantes sont supprimées et la carte est reformatée.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Initialisation d'une carte SD vFlash à l'aide de l'utilitaire de configuration d'iDRAC

Pour initialiser une carte SD vFlash à l'aide de l'utilitaire de configuration d'iDRAC :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Paramètres de port USB et média**.
   La page **Paramètres d'iDRAC. Paramètres de port USB et de média** s'affiche.
2. Cliquez sur **Initialiser vFlash**.
3. Cliquez sur **Oui**. L'initialisation démarre.
4. Cliquez sur **Retour** et accédez à la même page **Paramètres d'iDRAC. Paramètres de port USB** pour afficher le message d'aboutissement.
   Tout le contenu existant est supprimé et la carte est reformatée avec les nouvelles informations système vFlash.

Obtention du dernier état à l'aide de RACADM

Pour obtenir l'état de la dernière commande d'initialisation envoyée à la carte SD vFlash :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.

2. Entrez la commande `racadm vFlashsd status`
   L'état des commandes envoyées à la carte SD s'affiche.
3. Pour obtenir le dernier état de toutes les partitions vFlash, exécutez la commande `racadm vflashpartition status -a`
4. Pour obtenir le dernier état d'une partition, exécutez la commande `racadm vflashpartition status -i (index)`

   REMARQUE : Si iDRAC est réinitialisé, l'état de la dernière opération de partition est perdue.

Gestion des partitions vFlash

Vous pouvez exécuter les opérations suivantes dans l'interface Web d'iDRAC ou RACADM :

REMARQUE : Un administrateur peut exécuter toutes les opérations sur les partitions vFlash. Autrement, vous devez disposer du privilège d'**Accès au Média Virtuel** pour pouvoir créer, supprimer, formater, connecter ou copier le contenu de la partition.

- Création d'une partition vide
- Création d'une partition à l'aide d'un fichier image
- Formatage d'une partition
- Affichage des partitions disponibles
- Modification d'une partition
- Connexion et déconnexion de partitions
- Suppression de partitions existantes
- Téléchargement du contenu d'une partition
- Démarrage à partir d'une partition

REMARQUE : Si vous cliquez sur une option dans les pages vFlash lorsqu'une application telle que WSMAN, l'utilitaire de configuration d'iDRAC ou RACADM utilise vFlash ou si vous naviguez vers une autre page dans l'interface graphique, iDRAC affiche le message : `vFlash is currently in use by another process. Try again after some time.`

VFlash est capable de créer rapidement une partition lorsque aucune autre opération vFlash n'est en cours, telle que le formatage, la connexion de partitions, et ainsi de suite. Par conséquent, il est recommandé de créer toutes les partitions avant d'effectuer d'autres opérations de partition.

Création d'une partition vide

Une partition vide, lorsqu'elle est connectée au système, est similaire à un lecteur Flash USB vide. Vous pouvez créer des partitions vides sur la carte SD vFlash. Vous pouvez créer des partitions de type *Disquette* ou *Disque dur*. La partition de type CD est prise en charge uniquement lors de la création de partitions en utilisant des images.

Avant de créer une partition vide, vérifiez que :

- Vous disposez du privilège d'**Accès Média Virtuel**.
- La carte est initialisée.
- La carte n'est pas protégée contre l'écriture.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

Création d'une partition vide à l'aide de l'interface Web

Pour créer une partition vFlash vide :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Créer une partition vide**.
   La page **Créer une partition vide** s'affiche.
2. Entrez les informations nécessaires et cliquez sur **Appliquer**. Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC*.

   Une nouvelle partition vide non formatée est créée en lecture seule par défaut. Une page s'affiche pour indiquer le pourcentage d'avancement. Un message d'erreur s'affiche :
   - La carte est protégée contre l'écriture.
   - Le nom d'étiquette correspond à l'étiquette d'une partition existante.
   - Une valeur autre qu'un entier est entrée pour la taille de partition, la valeur dépasse l'espace disponible sur la carte ou la taille de partition est supérieure à 4 Go.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

Création d’une partition vide à l’aide de RACADM

Pour créer une partition vide :

1. Ouvrez une session sur le système à l’aide de telnet, de SSH, ou de la console série.
2. Entrez la commande :

```
racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s [n]
```

   où `[n]` est la taille de la partition.

   Par défaut, une partition vide lisible et inscriptible est créée.

Création d'une partition à l'aide d'un fichier image

Vous pouvez créer une partition sur la carte SD vFlash en utilisant un fichier image (disponible dans le format **.img** ou **.iso**.) Les partitions sont des types d’émulations : disquette (**.img**), disque dur (**.img**) ou CD (**.iso**). La taille de la partition créée est égale à la taille du fichier image.

Avant de créer une partition depuis un fichier image, vérifiez que :

- Vous disposez du privilège d'accès Média Virtuel.
- La carte est initialisée.
- La carte n'est pas protégée contre l'écriture.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

REMARQUE : L’image téléchargée et le type d’émulation doivent correspondre. Des problèmes apparaissent lorsqu’iDRAC émule un périphérique avec un type d’image incorrect. Par exemple, si la partition est créée à l’aide d’une image ISO et que le type d’émulation défini est Disque dur, le BIOS ne peut pas démarrer depuis cette image.

- Le type d'image et le type d'émulation correspondent.
- La taille de l'image est inférieure ou égale à l'espace disponible sur la carte.
- La taille du fichier image est inférieure ou égale à 4 Go, car la taille maximale d’une partition prise en charge est de 4 Go. Cependant, lors de la création d’une partition à l’aide d’un navigateur Web, le fichier image doit avoir une taille inférieure à 2 Go.

REMARQUE : La partition vFlash est un fichier image sur un système de fichiers FAT32. Par conséquent, le fichier image a une limite de 4 Go.

Création d'une partition à l'aide d'un fichier image et de l'interface Web

Pour créer une partition vFlash à l'aide d'un fichier image :

1. Dans l’interface Web d’iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Créer depuis une image**.
   La page de **Créer une partition depuis un fichier image** s'affiche.
2. Entrez les informations nécessaires et cliquez sur **Appliquer**. Pour plus d'informations sur les options, Voir l'*Aide en ligne d'iDRAC*.
   Une partition est créée. Pour le type d'émulation CD, une partition en lecture seule est crée. Pour le type d'émulation Disquette ou Disque dur, une partition lisible et inscriptible est créée. Un message d'erreur s'affiche si :
   - La carte est protégée contre l'écriture.
   - Le nom d'étiquette correspond à l'étiquette d'une partition existante.
   - La taille du fichier image est supérieure à 4 Go ou excède l'espace disponible sur la carte.
   - Le fichier image n'existe pas ou son extension n'est ni .img, ni .iso.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

Création d’une partition depuis un fichier image à l’aide de RACDAM

Pour créer une partition depuis un fichier image à l’aide de l’interface RACADM :

1. Ouvrez une session sur le système à l’aide de telnet, de SSH, ou de la console série.

2. Entrez la commande

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/
foo.iso -u root -p mypassword
```

Une partition est créée. Par défaut, elle est en lecture seule. Cette commande est sensible à la casse pour l'extension du nom de fichier de l'image. Si cette extension est en majuscules, par exemple FOO.ISO au lieu de FOO.iso, la commande renverra une erreur de syntaxe.

REMARQUE : Cette fonction n'est pas prise en charge dans l'interface RACADM locale.

REMARQUE : La création d'une partition vFlash depuis un fichier image situé sur un partage de réseau IPv6 CFS ou NFS IPv6 n'est pas prise en charge.

Formatage d'une partition

Vous pouvez formater une partition existante sur la carte SD vFlash en fonction du type de système de fichiers. Les types de systèmes de fichiers compatibles sont EXT2, EXT3, FAT16 et FAT32. Vous pouvez formater des partitions de type Disque dur ou Disquette, mais pas CD. Vous ne pouvez pas formater des partitions en lecture seule.

Avant de créer une partition depuis un fichier image, assurez-vous que :

- Vous disposez du privilège d'**accès Média Virtuel**.
- La carte est initialisée.
- La carte n'est pas protégée contre l'écriture.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

Pour formater la partition vFlash :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Formater**.
   La page **Formater la partition** s'affiche.
2. Saisissez les informations requises, puis cliquez sur **Appliquer**.
   Pour plus d'informations sur les options, voir l'*Aide en ligne d'iDRAC*.
   Un message d'avertissement s'affiche pour indiquer que toutes les données de la partition seront effacées.
3. Cliquez sur **OK**.
   La partition sélectionnée est formatée en fonction du type de système de fichiers défini. Un message d'erreur s'affiche si :
   - La carte est protégée contre l'écriture.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

Affichage des partitions disponibles

Vérifiez que la fonctionnalité vFlash est activée pour pouvoir afficher la liste des partitions disponibles.

Affichage des partitions disponibles à l'aide de l'interface Web

Pour afficher les partitions vFlash, dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Gérer**. La page **Gérer des partitions** s'affiche avec la liste des partitions disponibles et les informations de chaque partition. Pour en savoir plus sur les partitions, voir l'*Aide en ligne d'iDRAC*.

Affichage des partitions disponibles à l'aide de RACADM

Pour afficher les partitions disponibles et leurs propriétés en utilisant l'interface RACADM :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez les commandes suivantes :
   - Pour répertorier toutes les partitions existantes et leurs propriétés :

     ```
     racadm vflashpartition list
     ```

   - Pour obtenir l'état de fonctionnement de la partition 1 :

```
racadm vflashpartition status -i 1
```

- Pour obtenir l'état de toutes les partitions existantes :

```
racadm vflashpartition status -a
```

REMARQUE : L'option -a est valide uniquement avec l'option d'état.

Modification d'une partition

Vous pouvez convertir une partition en lecture seule en partition inscriptible et lisible et inversement. Avant de modifier la partition, vérifiez que :

- La fonctionnalité vFlash est activée.
- Vous disposez des privilèges d'**Accès Média Virtuel**.

REMARQUE : Par défaut, une partition en lecture seule est créée.

Modification d'une partition à l'aide de l'interface Web

Pour modifier des partitions :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Gérer**.
   La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Lecture seule** :
   - Cochez la case des partitions et cliquez sur **Appliquer** pour passer en lecture seule.
   - Cochez la case des partitions et cliquez sur **Appliquer** pour passer en lecture-écriture.

     Les partitions passent en lecture seule ou en lecture-écriture selon les sélections effectuées.

     REMARQUE : S'il s'agit d'une partition de type CD, l'état est Lecture seule. Vous ne pouvez pas remplacer l'état par lecture-écriture. Si la partition est connectée, la case est estompée.

Modification d'une partition à l'aide de RACADM

Pour afficher les partitions disponibles et leurs propriétés sur la carte :

1. Ouvrez une session sur le système à l'aide de telnet, de SSH, ou de la console série.
2. Procédez de l'une des manières suivantes :
   - Utilisation de la commande `set` pour modifier l'état de lecture/écriture de la partition :
     - Pour remplacer une partition en lecture seule par une partition en lecture-écriture :

       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 1
       ```

     - Pour remplacer une partition en lecture-écriture par une partition en lecture seule :

       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 0
       ```

   - Utilisation de la commande `set` pour définir le type d'émulation :

     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

Connexion et déconnexion de partitions

Lorsque vous connectez des partitions, elles sont accessibles au système d'exploitation et au BIOS comme périphériques de stockage de masse USB. Lorsque vous connectez plusieurs partitions en fonction de l'index affecté, elles sont répertoriées en ordre croissant dans le système d'exploitation et dans le menu de la séquence de démarrage BIOS.

Si vous déconnectez une partition, elle n'est pas accessible au système d'exploitation et elles ne figure pas dans le menu de la séquence de démarrage.

Lorsque vous connectez ou déconnectez une partition, le bus USB dan le système géré est réinitialisé. Ceci affecte les applications qui utilisent vFlash et déconnecte les sessions Média Virtuel iDRAC.

Avant de connecter ou de déconnecter une partition :

- La fonctionnalité vFlash est activée.
- Vérifiez qu'aucune opération d'initialisation n'est en cours d'exécution sur la carte.
- Vérifiez que vous disposez des privilèges **d'accès Média Virtuel**.

Connexion et déconnexion de partitions à l'aide de l'interface Web

Pour connecter ou déconnecter des partitions :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Gérer**.
   La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Connecté** :
   - Cochez la case de la ou des partitions et cliquez sur **Appliquer** pour connecter les partitions.
   - Désélectionnez la case de la ou des partitions et cliquez sur **Appliquer** pour déconnecter les partitions.

     Les partitions sont connectées ou déconnectées en fonction des sélections effectuées.

Connexion ou déconnexion de partitions à l’aide de l’interface RACADM

Pour connecter ou déconnecter des partitions :

1. Ouvrez une session sur le système à l’aide de telnet, de SSH, ou de la console série.
2. Utilisez les commandes suivantes :
   - Pour connecter une partition :

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 1
     ```

   - Pour déconnecter une partition :

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 0
     ```

Comportement du système d'exploitation pour les partitions connectées

Pour les systèmes d'exploitation Windows et Linux :

- Le système d'exploitation contrôle les lettres de lecteur et les affecte aux partitions connectées.
- Les partitions en lecture seule sont des lecteurs en lecture seule dans le système d'exploitation.
- Le système d'exploitation doit prendre en charge le système de fichiers d'une partition connectée pour qu'il puisse lire ou modifier le contenu de la partition. Par exemple, dans un environnement Windows, le système d'exploitation ne peut pas lire une partition de type EXT2 qui est native dans Linux. En outre, dans un environnement Linux, le système d'exploitation ne peut pas lire une partition de type NTFS qui est native dans Windows.
- L'étiquette de partition vFlash est différente du nom de volume du système de fichiers sur le lecteur émulé USB. Vous pouvez changer le nom de volume du lecteur émulé USB depuis le système d'exploitation. Cependant, cette modification ne change pas le nom d'étiquette de partition stocké dans iDRAC.

Suppression de partitions existantes

Avant de supprimer des partitions, vérifiez que :

- La fonctionnalité vFlash est activée.
- La carte n'est pas protégée contre l'écriture.
- La partition n'est pas connectée.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.

Suppression de partitions existantes à l'aide de l'interface Web

Pour supprimer une partition existante :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Gérer**.
   La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Supprimer**, cliquez sur l'icône de suppression de la partition à supprimer.
   Un message s'affiche pour indiquer que l'action va supprimer définitivement la partition.
3. Cliquez sur **OK**.
   La partition est supprimée.

Suppression de partitions à l'aide de RACADM

Pour supprimer des partitions :

1. Ouvrez une console Telnet, SSH ou série sur le système et ouvrez une session.
2. Entrez les commandes suivantes :
   - Pour supprimer une partition :

     ```
     racadm vflashpartition delete -i 1
     ```

   - Pour supprimer toutes les partitions, réinitialisez la carte SD vFlash.

Téléchargement du contenu d'une partition

Vous pouvez télécharger le contenu d'une partition vFlash dans le format **.img** ou **.iso** :

- sur le système géré (d'où iDRAC est exécuté) ;
- dans l'emplacement réseau mappé à une station de gestion.

Avant de télécharger le contenu de la partition, vérifiez que :

- Vous disposez des privilèges d'accès à Média Virtuel.
- La fonctionnalité vFlash est activée.
- Une opération d'initialisation n'est pas en cours d'exécution sur la carte.
- S'il s'agit d'une partition en lecture-écriture, elle ne doit pas être connectée.

Pour télécharger le contenu de la partition vFlash :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **vFlash** > **Télécharger**.
   La page **Télécharger la partition** s'affiche.
2. Dans le menu déroulant **Nom**, sélectionnez la partition à télécharger et cliquez sur **Télécharger**.

   REMARQUE : Toutes les partitions existantes (à l'exception des partitions connectées) s'affichent dans la liste. La première partition est la partition par défaut.

3. Spécifiez l'emplacement d'enregistrement du fichier.
   Le contenu de la partition sélectionnée est téléchargé vers l'emplacement spécifié.

   REMARQUE : Si vous définissez uniquement l'emplacement du dossier, le nom de la partition est utilisé comme nom de fichier avec l'extension **.iso** pour les types de partitions CD et Disque dur, et **.img** pour les types de partitions Disquette et Disque dur.

Démarrage à partir d'une partition

Vous pouvez définir une partition vFlash connectée en tant que périphérique de démarrage pour le démarrage suivant.

Avant de démarrer dans une partition,vérifiez que :

- La partition vFlash contient une image amorçable (de format **.img** ou **.iso**) à démarrer depuis le périphérique.
- La fonctionnalité vFlash est activée.
- Vous disposez des privilèges d'accès à Média Virtuel.

Démarrage depuis une partition à l'aide de l'interface Web

Pour définir la partition vFlash comme premier périphérique de démarrage, voir Définition du premier périphérique de démarrage.

REMARQUE : Si la ou les partitions vFlash connectées ne figurent pas dans le menu déroulant **Premier périphérique de démarrage**, vérifiez que vous disposez de la dernière version du BIOS.

Démarrage à partir d'une partition à l'aide de RACADM

Pour définir une partition vFlash en tant que le premier périphérique de démarrage, utilisez l'objet `iDRAC.ServerBoot`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

REMARQUE : Lorsque vous exécutez la commande, l'étiquette de partition vFlash est définie automatiquement pour un démarrage ponctuel ; `iDRAC.ServerBoot.BootOnce` est défini à `1`. Dans ce cas, le périphérique démarre une seule fois dans la partition et, après cela, ne reste pas le premier périphérique de la séquence de démarrage.

18

Utilisation de SMCLP

La spécification SMCLP (Server Management Command Line Protocol) permet de gérer les systèmes CLI. Elle définit un protocole pour les commandes de gestion envoyées dans des flux orientés caractère standard. Ce protocole accède à un Gestionnaire CIMOM (Common Information Model Object Manager) en utilisant un groupe de commandes manuelles. SMCLP est un sous-composant du projet SMASH DMTF (Distributed Management Task Force) pour rationaliser la gestion des systèmes sur plusieurs plates-formes. La spécification SMCLP, et la spécification Managed Element Addressing Specification et de nombreux profils dans les spécifications de mappage SMCLP, décrit les verbes et les cibles standard pour les exécutions de tâches de gestion.

REMARQUE : Elle suppose que vous connaissez le projet SMASH (Systems Management Architecture for Server Hardware) et les spécifications SMCLP SMWG (Server Management Working Group).

SM-CLP est un sous-composant du projet SMASH DMTF (Distributed Management Task Force) pour rationaliser la gestion des serveurs sur plusieurs plate-formes. La spécification SM-CLP, et la spécification MEAS (Managed Element Addressing Specification) et les nombreux profils dans les spécifications SM-CLP, décrit les verbes et les cibles standard des exécutions de tâches de gestion.

SMCLP est hébergé depuis le micrologiciel du contrôleur iDRAC et prend en charge les interfaces Telnet, SSH et série. L'interface SMCLP iDRAC repose sur la spécification SMCLP 1.0 fournie par l'organisation DMTF.

REMARQUE : Des informations sur les profils, les extensions et les MOF sont disponibles sur **delltechcenter.com** et toutes les informations DMTF sont disponibles sur **dmtf.org/standards/profiles/**.

Les commandes SM-CLP mettent en œuvre un sous-ensemble de commandes RACADM. Les commandes sont pratiques pour le scriptage, puisque vous pouvez les exécuter depuis une ligne de commande de station de gestion. Vous pouvez extraire la sortie des commandes dans des formats bien définis, notamment XML, ce qui facilite le scriptage et l'intégration aux outils de génération de rapport et de gestion.

Sujets :

- Fonctions de gestion de système à l'aide de SMCLP
- Exécution des commandes SMCLP
- Syntaxe SMCLP iDRAC
- Navigation dans l'espace d'adressage MAP
- Utilisation du verbe show
- Exemples d'utilisation

Fonctions de gestion de système à l'aide de SMCLP

SMCLP iDRAC permet de :

- Gérer l'alimentation du serveur : mise sous tension, arrêt ou redémarrage du système
- Gérer le journal des événements système (SEL) : affichage ou effacement des enregistrements du journal SEL
- Gérer le compte d'utilisateur iDRAC
- Afficher les propriétés du système

Exécution des commandes SMCLP

Vous pouvez exécuter les commandes SMCLP à l'aide d'une interface SSH ou Telnet. Ouvrez une interface SSH ou Telnet et ouvrez une session dans iDRAC comme administrateur. L'invite SMCLP (admin ->) s'affiche.

Invites SMCLP :

- serveurs lames yx1x, utilisez `-$`.
- serveurs en rack et de type tour yx1x, utilisez `admin->`.
- serveurs lames, en rack et de type tour yx2x, utilisez `admin->`.

, où y est un caractère alphanumérique tel que M (pour serveurs lames), R (pour serveurs en rack) et T (pour les serveurs de type tour) et x est un nombre. Ceci indique la génération des serveurs Dell PowerEdge.

REMARQUE : Les scripts qui utilisent `-$` peuvent utiliser ces données pour les systèmes yx1x, mais à partir des systèmes yx2x un script avec `admin->` peut être utilisé pour les serveurs lames, en rack et de type tour.

Syntaxe SMCLP iDRAC

SMCLPP iDRAC utilise le concept de verbe et de cible pour fournir des fonctions de gestion de systèmes via l'interface CLI. Un verbe indique l'opération à exécuter et une cible détermine l'entité (ou l'objet) qui exécute l'opération.

Syntaxe de ligne de commande SMCLP :

```
<verb> [<options>] [<target>] [<properties>]
```

Le tableau suivant répertorie les verbes et leur définition.

Tableau 43. Verbes SMCLP

Verbe	Définition
cd	Navigue dans MAP à l'aide de l'environnement
set	Affecte une valeur à une propriété
aide	Affiche l'aide d'une cible
reset	Réinitialise une cible
show	Affiche les propriétés, les verbes et les sous-cibles d'une cible
start	Active une cible
stop	Arrête une cible
exit	Quitte la session dans l'environnement SMCLP
version	Affiche les attributs de version d'une cible
load	Transfère une image binaire d'une URL vers une adresse cible spécifiée

Le tableau suivant répertorie les cibles.

Tableau 44. Cibles SMCLP

Cible	Définitions
`admin1`	domaine admin
`admin1/profiles1`	Profils enregistrés dans iDRAC
`admin1/hdwr1`	Matériel
`admin1/system1`	Cible du système géré
`admin1/system1/capabilities1`	Fonctions de collecte SMASH du système géré
`admin1/system1/capabilities1/pwrcap1`	Fonctions d'utilisation de l'alimentation du système géré

Tableau 44. Cibles SMCLP (suite)

Cible	Définitions
`admin1/system1/capabilities1/elecap1`	Fonctions de cible du système géré
`admin1/system1/logs1`	Cible des collectes du journal d'enregistrements
`admin1/system1/logs1/log1`	Entrée d'enregistrement du journal des événements système (SEL)
`admin1/system1/logs1/log1/record*`	Instance d'enregistrement SEL individuelle sur le système géré
`admin1/system1/settings1`	Paramètres de collecte SMASH du système géré
`admin1/system1/capacities1`	Collecte SMASH des capacités du système géré
`admin1/system1/consoles1`	Collecte SMASH des consoles du système géré
`admin1/system1/sp1`	Processeur de service
`admin1/system1/sp1/timesvc1`	Service de temps du processeur de service
`admin1/system1/sp1/capabilities1`	Collecte SMASH des capacités du processeur de service
`admin1/system1/sp1/capabilities1/clpcap1`	Fonctions de service CLP
`admin1/system1/sp1/capabilities1/pwrmgtcap1`	Fonctions de service de gestion de l'état de l'alimentation sur le système
`admin1/system1/sp1/capabilities1/acctmgtcap*`	Fonctions de service de gestion de comptes
`admin1/system1/sp1/capabilities1/rolemgtcap*`	Fonctions de gestion basées sur les rôles locaux
`admin1/system1/sp1/capabilities/PwrutilmgtCap1`	Fonctions de gestion de l'utilisation de l'alimentation
`admin1/system1/sp1/capabilities1/elecap1`	Fonctions d'authentification
`admin1/system1/sp1/settings1`	Collecte des paramètres du processeur de service
`admin1/system1/sp1/settings1/clpsetting1`	Données des paramètres de service CLP
`admin1/system1/sp1/clpsvc1`	Service de protocole de service CLP

Tableau 44. Cibles SMCLP (suite)

Cible	Définitions
`admin1/system1/sp1/clpsvc1/clpendpt*`	Terminaison de protocole de service CLP
`admin1/system1/sp1/clpsvc1/tcpendpt*`	Terminaison TCP de protocole de service CLP
`admin1/system1/sp1/jobq1`	File d'attente des tâches du protocole de service CLP
`admin1/system1/sp1/jobq1/job*`	Tâche du protocole de service CLP
`admin1/system1/sp1/pwrmgtsvc1`	Service de gestion de l'état de l'alimentation
`admin1/system1/sp1/account1-16`	Compte d'utilisateur local
`admin1/sysetm1/sp1/account1-16/identity1`	Compte d'identité d'utilisateur local
`admin1/sysetm1/sp1/account1-16/identity2`	Compte d'identité IPMI (LAN)
`admin1/sysetm1/sp1/account1-16/identity3`	Compte d'identité IPMI (série)
`admin1/sysetm1/sp1/account1-16/identity4`	Compte d'identité CLP
`admin1/system1/sp1/acctsvc1`	Service de gestion de compte d'utilisateur local
`admin1/system1/sp1/acctsvc2`	Service de gestion de compte IPMI
`admin1/system1/sp1/acctsvc3`	Service de gestion de compte CLP
`admin1/system1/sp1/rolesvc1`	Service d'autorisation basée sur des rôles (RBA) locaux
`admin1/system1/sp1/rolesvc1/Role1-16`	Rôle local
`admin1/system1/sp1/rolesvc1/Role1-16/privilege1`	Privilège de rôle local
`admin1/system1/sp1/rolesvc2`	Service RBA IPMI
`admin1/system1/sp1/rolesvc2/Role1-3`	Rôle IPMI
`admin1/system1/sp1/rolesvc2/Role4`	Rôle Série sur LAN (SOL) IPMI

Tableau 44. Cibles SMCLP (suite)

Cible	Définitions
`admin1/system1/sp1/rolesvc3`	Service RBA CLP
`admin1/system1/sp1/rolesvc3/Role1-3`	Rôle CLP
`admin1/system1/sp1/rolesvc3/Role1-3/privilege1`	Privilège de rôle CLP

Concepts associés

Exécution des commandes SMCLP , page 267
Exemples d'utilisation , page 272

Navigation dans l'espace d'adressage MAP

Les objets qui peuvent être gérés avec SM-CLP sont représentés par des cibles organisées dans un espace hiérarchique appelé espace d'adressage MAP (Manageability Access Point). Un chemin d'adressage définit le chemin de la racine de l'espace d'adressage vers un objet dans l'espace d'adresse.

La cible racine est représentée par une barre oblique (`/`) ou une barre oblique inverse (`\`). Il s'agit du point de départ par défaut lorsque vous ouvrez une session dans iDRAC. Accédez à la racine en utilisant le verbe `cd`.

REMARQUE : La barre oblique (`/`) et la barre oblique inverse (`\`) sont permutables dans les chemins d'adressage SM-CLP. Toutefois, une barre oblique inverse à la fin d'une ligne de commande continue la commande sur la ligne suivante et elle est ignorée lorsque la commande est analysée.

Par exemple, pour accéder au troisième enregistrement du journal des événements système (SEL), entrez la commande suivante :

```
->cd /admin1/system1/logs1/log1/record3
```

Entrez le verbe `cd` sans cible pour rechercher votre emplacement actuel dans l'espace d'adressage. Les abréviations `..` et `.` fonctionnent comme dans Windows et Linux : `..` fait référence au niveau parent et `.` au niveau actuel.

Utilisation du verbe show

Pour en savoir plus sur une cible, utilisez le verbe `show`. Ce verbe permet d'afficher les propriétés de la cible, des sous-cibles, des associations et la liste des verbes SM-CLP autorisés dans l'emplacement.

Utilisation de l'option -display

L'option `show -display` permet de limiter la sortie de la commande à une ou plusieurs propriétés, cibles, associations et un ou plusieurs verbes. Par exemple, pour afficher uniquement les propriétés et les cibles dans l'emplacement actuel, utilisez la commande suivante :

```
show -display properties,targets
```

Pour répertorier uniquement certaines propriétés, qualifiez-les, comme dans la commande suivante :

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

Si vous souhaitez uniquement afficher une propriété, vous pouvez omettre les parenthèses.

Utilisation de l'option -level

L'option `show -level` exécute `show` sur les niveaux supplémentaires sous la cible définie. Pour afficher toutes les cibles et les propriétés dans l'espace d'adressage, utilisez l'option `-l all`.

Utilisation de l'option -output

L'option `-output` spécifie l'un des quatre formats de sortie suivants pour les verbes SM-CLP : **texte**, **clpcsv**, **keyword** et **clpxml**.

Le format par défaut **text** est le plus lisible. Le format **clpcsv** est un format de valeurs séparées par une virgule à charger dans un tableur. Le format **keyword** génère des informations dans une liste de paires keyword=value avec une paire sur chaque ligne. Le format **clpxml** est un document XML qui contient un élément XML **response**. DMTF a défini les formats **clpcsv** et **clpxml** et leurs spécifications sont disponibles sur le site Web DMTF, **dmtf.org**.

L'exemple suivant montre comment générer le contenu du journal SEL dans le format XML :

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Exemples d'utilisation

Cette section fournit des scénarios de cas d'utilisation pour SMCLP:

- Gestion de l'alimentation du serveur
- Gestion du journal SEL
- Navigation dans la cible MAP

Gestion de l'alimentation du serveur

Les exemples suivants expliquent comment utiliser SMCLP pour exécuter des opérations de gestion de l'alimentation sur un système géré.

Tapez les commandes suivantes dans l'invite de commande SMCLP :

- Pour arrêter le serveur :

  ```
  stop /system1
  ```

  Le message suivant s'affiche :

  ```
  system1 has been stopped successfully
  ```

- Pour démarrer le serveur :

  ```
  start /system1
  ```

  Le message suivant s'affiche :

  ```
  system1 has been started successfully
  ```

- Pour redémarrer le serveur :

  ```
  reset /system1
  ```

  Le message suivant s'affiche :

  ```
  system1 has been reset successfully
  ```

Gestion du journal SEL

Les exemples suivants expliquent comment utiliser SMCLP pour exécuter des opérations liées au SEL sur le système géré. Tapez les commandes suivantes dans l'invite de commande SMCLP :

- Pour afficher le journal SEL :

  ```
  show/system1/logs1/log1
  ```

  La sortie suivante s'affiche :

  ```
  /system1/logs1/log1
  Targets:
  Record1
  Record2
  Record3
  ```

```
Record4
Record5
Properties:
InstanceID = IPMI:BMC1 SEL Log
MaxNumberOfRecords = 512
CurrentNumberOfRecords = 5
Name = IPMI SEL
EnabledState = 2
OperationalState = 2
HealthState = 2
Caption = IPMI SEL
Description = IPMI SEL
ElementName = IPMI SEL
Commands:
cd
show
help
exit
version
```

- Pour afficher l'enregistrement SEL :

  ```
  show/system1/logs1/log1
  ```

  La sortie suivante s'affiche :

  ```
  /system1/logs1/log1/record4
  Properties:
  LogCreationClassName= CIM_RecordLog
  CreationClassName= CIM_LogRecord
  LogName= IPMI SEL
  RecordID= 1
  MessageTimeStamp= 20050620100512.000000-000
  Description= FAN 7 RPM: fan sensor, detected a failure
  ElementName= IPMI SEL Record
  Commands:
  cd
  show
  help
  exit
  version
  ```

- Pour effacer le journal SEL :

  ```
  delete /system1/logs1/log1/record*
  ```

  La sortie suivante s'affiche :

  ```
  All records deleted successfully
  ```

Navigation dans la cible MAP

Les exemples suivants montrent comment utiliser le verbe cd pour naviguer dans MAP. Dans tous les exemples, la cible par défaut initiale est supposée être `/`.

Tapez les commandes suivantes dans l'invite de commande SMCLP :

- Pour accéder à la cible système et redémarrer :

  cd system1 reset. La cible par défaut actuelle est `/`.

- Pour accéder à la cible SEL et afficher les enregistrements du journal :

  ```
  cd system1
  cd logs1/log1
  show
  ```

- Pour afficher la cible en cours :

  type `cd .`

- Pour monter d'un niveau :

  type `cd ..`

- Pour quitter :

  ```
  exit
  ```

19

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 fonctionner avec des interfaces iDRAC telles que les interfaces Web, RACADM et WSMAN. Vous pouvez configurer les fonctionnalités surveillées par l'iDRAC Service Module pour contrôler l'UC et la mémoire utilisée sur le système d'exploitation du serveur.

REMARQUE : Vous pouvez utiliser l'iDRAC Service Module uniquement si vous avez installé une licence de contrôleur iDRAC Express ou iDRAC Enterprise.

Avant d'utiliser l'iDRAC Service Module, assurez-vous que :

- Vous disposez de privilèges de connexion, de configuration et de contrôle de serveur dans 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 de l'OS à iDRAC est activé par l'intermédiaire du bus USB interne dans l'iDRAC.

REMARQUE :

- Lorsque l'iDRAC Service Module s'exécute pour la première fois, il active par défaut la connexion directe entre le système d'exploitation et l'iDRAC dans iDRAC. Si vous désactivez cette fonction après l'installation de l'iDRAC Service Module, vous devez l'activer manuellement dans l'iDRAC.
- Si la connexion directe entre le système d'exploitation et l'iDRAC est activée via le LOM dans iDRAC, vous ne pouvez pas utiliser l'iDRAC Service Module.

Sujets :

- Installation de l'iDRAC Service Module
- Systèmes d'exploitation pris en charge de l'iDRAC Service Module
- Fonctionnalités de surveillance de l'iDRAC Service Module
- Utilisation de l'iDRAC Service Module à partir de l'interface Web iDRAC
- Utilisation de l'iDRAC Service Module à l'aide de RACADM
- Utilisation d'iDRAC Service Module d'iDRAC sur Windows Nano

Installation de l'iDRAC Service Module

Vous pouvez télécharger et installer l'iDRAC Service Module (Module de service iDRAC) depuis le site **dell.com/support**. Vous devez disposer de privilèges administrateurs sur le système d'exploitation du serveur pour installer l'iDRAC Service Module (Module de service iDRAC). Pour en savoir plus sur l'installation, voir l'*iDRAC Service Module User's Guide* (Guide d'utilisation du module Service iDRAC) disponible à l'adresse **dell.com/support/manuals**.

REMARQUE : Cette fonctionnalité ne s'applique pas aux systèmes Dell Precision PR7910.

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 l'*iDRAC Service Module Installation Guide* (Guide d'installation de l'iDRAC Service Module) disponible à l'adresse **dell.com/openmanagemanuals**.

Fonctionnalités de surveillance de l'iDRAC Service Module

L'iDRAC Service Module (iSM) offre les fonctionnalités de surveillance suivantes :

- Prise en charge de profil Redfish pour les attributs réseau
- Réinitialisation matérielle d'iDRAC
- Accès à iDRAC via l'OS hôte (fonctionnalité expérimentale)
- Alertes SNMP intrabande de l'iDRAC
- Afficher 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
- Remplir les fournisseurs de gestion WMI (Windows Management Instrumentation)
- Intégration à la collection SupportAssist. Cela s'applique uniquement si l'iDRAC Service Module version 2.0 ou ultérieure est installé. Pour en savoir plus, voir la section Generating SupportAssist Collection (Génération de la collecte SupportAssist).
- Préparation au retrait du périphérique SSD PCIe NVMe Pour plus d'informations, reportez-vous à Idracug_preparing to remove nvme pcie ssd.

REMARQUE : Les fonctionnalités, telles que Windows Management Instrumentation Providers, la Préparation au retrait d'un périphérique SSD PCIe NVMe par le biais de l'iDRAC, l'Automatisation de la collecte du système d'exploitation pour la collecte pour SupportAssist sont prises en charge uniquement sur les serveurs Dell PowerEdge de13e génération dont la version micrologicielle minimale est 2.00.00.00 ou une version ultérieure.

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.

Informations sur le système d'exploitation

OpenManage Server Administrator partage actuellement les informations sur le système d'exploitation et le nom d'hôte avec l'iDRAC. L'iDRAC Service Module fournit les mêmes informations telles que le nom du système d'exploitation, la version du système d'exploitation et le nom de domaine complet (FQDN) avec iDRAC. Par défaut, cette fonctionnalité de surveillance est activée. Elle n'est pas désactivée si OpenManage Server Administrator est installé sur le système d'exploitation hôte.

L'iDRAC Service Module version 2.0 ou ultérieure a modifié la fonction d'informations sur le système d'exploitation à l'aide de la surveillance de l'interface réseau de l'OS. Lorsque l'iDRAC Service Module version 2.0 ou ultérieure est utilisé avec l'iDRAC 2.00.00.00, il commence à surveiller les interfaces réseau du système d'exploitation. Vous pouvez afficher ces informations à l'aide de l'interface Web de l'iDRAC ou des interfaces RACADM ou WSMAN. Pour plus d'informations, voir Viewing network interfaces available on host os (Affichage des interfaces réseau disponibles sur l'OS hôte).

Lorsque l'iDRAC Service Module version 2.0 ou ultérieure est utilisé avec une version d'iDRAC antérieure à 2.00.00.00, la fonction d'informations sur l'OS ne fournit pas de surveillance de l'interface réseau de l'OS.

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 les interfaces équivalentes RACADM ou WSMAN) 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 : En commençant par l'iDRAC Service Module version 2.1, l'emplacement de réplication des journaux Lifecycle Controller dans les journaux du système d'exploitation Windows peut être configuré à l'aide du programme d'installation de l'iDRAC

Service Module. Vous pouvez configurer l'emplacement lors de l'installation de l'iDRAC Service Module ou la modification du programme d'installation de celui-ci.

Si OpenManage Server Administrator est installé, cette fonctionnalité de surveillance est désactivée pour éviter les doublons d'entrées du journal SEL dans le journal du système d'exploitation.

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, le moniteur d'intégrité peut ne pas être appelé, 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 de signal « heartbeat » (ou à pulsation) 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.

Fournisseurs WMI (Windows Management Instrumentation)

WMI est un ensemble d'extensions du modèle de pilotes Windows offrant une interface de système d'exploitation par laquelle les composants instrumentés fournissent des informations et des notifications. WMI est l'implémentation par Microsoft des normes Web-Based Enterprise Management (WBEM) et Common Information Model (CIM) publiées par le consortium DMTF (Distributed Management Task Force) pour gérer le matériel, les systèmes d'exploitation et les applications des serveurs. Les fournisseurs WMI participent à l'intégration avec les consoles de gestion des systèmes telles que Microsoft System Center et activent l'écriture de scripts de gestion des serveurs Microsoft Windows.

Vous pouvez activer ou désactiver l'option WMI dans l'iDRAC. L'iDRAC expose les classes de WMI via l'iDRAC Service Module qui fournit des informations sur l'intégrité du serveur. Par défaut, la fonction d'informations sur WMI est activée. L'iDRAC Service Module expose les classes surveillées par WSMAN dans iDRAC via WMI. Les classes sont présentées dans l'espace de nom `root/cimv2/dcim`.

Les classes sont accessibles via l'une des interfaces client WMI standard. Pour en savoir plus, voir les documents de profil.

Les exemples suivants utilisent la classe DCIM_account pour illustrer la capacité que fournit la fonction d'informations sur WMI dans l'iDRAC Service Module. Pour obtenir plus d'informations sur les classes et profils pris en charge, voir la documentation sur les profils WSMAN disponible dans le Dell TechCenter.

Tableau 45. Exemples

Interface CIM	WinRM	WMIC	PowerShell
Énumérer les instances d'une classe	`winrm e wmi/root/cimv2/dcim/dcim_account`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account`	`Get-WmiObject dcim_account -namespace root/cimv2/dcim`
Obtenir une instance particulière d'une classe	`winrm g wmi/root/cimv2/dcim/DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name="iDRAC.Embedded.1#Users.16"`	`Get-WmiObject -Namespace root\cimv2\dcim -Class dcim_account -filter "Name='iDRAC.Embedded.1#Users.16'"`

Tableau 45. Exemples (suite)

Interface CIM	WinRM	WMIC	PowerShell
Obtenir des instances associées à une instance	`winrm e wmi/root/cimv2/dcim/* -dialect:association -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name='iDRAC.Embedded.1#Users.2' ASSOC`	`Get-Wmiobject -Query "ASSOCIATORS OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`
Obtenir les références d'une instance	`winrm e wmi/root/cimv2/dcim/* -dialect:association -associations -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	Sans objet	`Get-Wmiobject -Query "REFERENCES OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`

Réinitialisation matérielle d'iDRAC à distance

À l'aide d'iDRAC, vous pouvez surveiller les serveurs pris en charge à la recherche des problèmes critiques liés au matériel, au micrologiciel, ou aux logiciels du système. Parfois, l'iDRAC peut ne pas répondre pour plusieurs raisons. Pendant ces scénarios, vous devez mettre le serveur hors tension et réinitialiser l'iDRAC. Pour réinitialiser l'UC de l'iDRAC, vous devez soit procéder à la mise hors tension et sous tension du serveur, soit effectuer un cycle d'alimentation en CA.

Avec la fonction de réinitialisation matérielle d'iDRAC à distance, à chaque fois que l'iDRAC ne répond plus, vous pouvez effectuer une opération de réinitialisation de l'iDRAC à distance sans effectuer un cycle d'alimentation en CA. Pour réinitialiser l'iDRAC à distance, vous devez disposer de privilèges administrateur sur le système d'exploitation de l'hôte. Par défaut, la fonction de réinitialisation matérielle d'iDRAC à distance est activée. Vous pouvez effectuer une réinitialisation matérielle distante d'iDRAC à l'aide de l'interface web iDRAC, RACADM et WSMAN.

REMARQUE : Cette fonction n'est pas prise en charge sur le serveur Dell PowerEdge R930 et est prise en charge uniquement sur les serveurs Dell PowerEdge de 13e génération et ultérieurs.

Utilisation des commandes

Cette section présente l'utilisation des commandes des systèmes d'exploitation Windows, Linux et ESXi pour exécuter la réinitialisation matérielle d'iDRAC.

- **Windows**
  - À l'aide de l'infrastructure Windows Management Instrumentation (WMI) locale :

    ```
    winrm  i  iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions"
    ```

  - À l'aide de l'interface WMI à distance :

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice -u:<admin-username> -p:<admin-
    passwd> -r: http://<remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck
    -skipCNCheck
    ```

- À l'aide du script Windows PowerShell avec force et sans force :

```
Invoke-iDRACHardReset -force
```

```
Invoke-iDRACHardReset
```

- À l'aide du raccourci dans le **menu Programmes** :

  Pour plus de simplicité, iSM fournit un raccourci dans le **menu Programmes** du système d'exploitation Windows. Lorsque vous sélectionnez l'option **Remote iDRAC Hard Reset (Réinitialisation matérielle d'iDRAC à distance)**, vous êtes invité à saisir une confirmation pour réinitialiser l'iDRAC. Une fois que vous avez confirmé, l'iDRAC est réinitialisé et le résultat de l'opération s'affiche.

REMARQUE : Le message d'avertissement suivant apparaît dans l'**Observateur d'événements** sous la catégorie **Journaux d'applications**. Cet avertissement ne nécessite aucune action supplémentaire.

```
A provider, ismserviceprovider, has been registered in the Windows Management
Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This account
is privileged and the provider may cause a security violation if it does not correctly
impersonate user requests.
```

- **Linux**

  iSM fournit une commande exécutable sur tous les systèmes d'exploitation Linux pris en charge par iSM. Vous pouvez exécuter cette commande en vous connectant au système d'exploitation avec SSH ou un équivalent.

```
Invoke-iDRACHardReset
```

```
Invoke-iDRACHardReset -f
```

- **ESXi**

  Sur tous les systèmes d'exploitation ESXi compatibles avec iSM, iSM v2.3 prend en charge un fournisseur de méthode CMPI (Common Management Programming Interface) pour exécuter la réinitialisation d'iDRAC à distance à l'aide des commandes à distance WinRM.

```
winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/
DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=
iSMExportedFunctions -u:<root-username> -p:<passwd> -r:https://<Host-IP>:443/wsman -
a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck
```

REMARQUE : Le système d'exploitation VMware ESXi ne demande pas de confirmation avant de réinitialiser l'iDRAC.

REMARQUE : En raison des limitations sur le système d'exploitation VMware ESXi, la connectivité de l'iDRAC n'est pas restaurée complètement après la réinitialisation. Assurez-vous de réinitialiser manuellement l'iDRAC. Pour plus d'informations, consultez la section « Réinitialisation matérielle d'iDRAC à distance » dans ce document.

Gestion d'erreurs

Tableau 46. Gestion d'erreurs

Résultat	Description
0	Succès
1	Version du BIOS non prise en charge pour la réinitialisation d'iDRAC
2	Plateforme non prise en charge
3	Accès refusé
4	La réinitialisation de l'iDRAC a échoué

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 de l'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 fonction 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 Windows**
  - À l'aide de l'infrastructure Windows Management Instrumentation (WMI) locale :

    ```
    winrm i EnableInBandSNMPTraps
    wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    ```

  - À l'aide de l'interface WMI à distance :

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    -u:<admin-username> -p:<admin-passwd> -r:http://<remote-hostname OR IP>/wsman  -a:Basic
    -encoding:utf-8 -skipCACheck -skipCNCheck
    ```

- **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 le Net-SNMP pour transférer les interruptions. Vous devez cependant configurer la destination d'interruption.

- **Système d'exploitation VMware ESXi**

Sur tous les systèmes d'exploitation ESXi compatibles avec iSM, iSM v2.3 prend en charge un fournisseur de méthode CMPI (Common Management Programming Interface) pour activer cette fonction à distance à l'aide des commandes à distance WinRM.

```
winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/
dcim/DCIM_iSMService?
__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<user-name> -p:<passwd> -
r:https://<remote-host-name
```

```
ip-address>:443/wsman -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -
skipRevocationcheck @{state="[0/1]"}
```

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 **In-Band SNMP Alerts** disponible sur **http://en.community.dell.com/techcenter/extras/m/white_papers**.

Accès à iDRAC via l'OS hôte (fonctionnalité expérimentale)

En utilisant cette fonctionnalité, vous pouvez configurer et surveiller les paramètres matériels via l'interface web iDRAC, WSMAN et Redfish, à l'aide de l'adresse IP de l'hôte sans configurer l'adresse IP de l'iDRAC. Vous pouvez utiliser les identifiants iDRAC par défaut si le serveur iDRAC n'est pas configuré ou continuer à utiliser les mêmes identifiants 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.
- Configurer 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 dans la plage 1024 à 65535. iSM redirige la connexion vers l'iDRAC. iSM crée ensuite une règle de pare-feu pour le trafic entrant, OS2iDRAC. Le numéro de port d'écoute est ajouté à la règle de pare-feu OS2iDRAC dans le système d'exploitation de l'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 de l'iDRAC, utilisez le format `https://<host-name>` ou `OS-IP>:443/login.html` dans le navigateur, où :

- `<host-name>` est le nom d'hôte complet du serveur sur lequel iSM est installé et configuré pour l'accès à iDRAC via la fonction du système d'exploitation. Vous pouvez utiliser l'adresse IP du système d'exploitation si le nom d'hôte n'est pas présent.
- `443` est la valeur par défaut du numéro de port d'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 iDRAC, WSMAN et 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 de l'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 fonction 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 :

```
Enable-iDRACAccessHostRoute get-status
```

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

Disable (mettre hors service)

`<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 dans *<IP-Address/subnet-mask>* format. Exemple : 10.95.146.98/24

Coexistence d'OpenManage Server Administrator et de l'iDRAC Service Module

Dans un système, OpenManage Server Administrator et l'iDRAC Service Module peuvent tous deux coexister et continuer de fonctionner correctement et de manière indépendante.

Si vous avez activé les fonctions de surveillance iDRAC au cours de l'installation de l'iDRAC Service Module, une fois l'installation terminée, si l'iDRAC Service Module détecte la présence d'OpenManage Server Administrator, il désactive l'ensemble de fonctionnalités de surveillance qui se chevauchent. Si OpenManage Server Administrator est en cours d'exécution, l'iDRAC Service Module désactive les fonctionnalités de surveillance qui se chevauchent après avoir ouvert une session sur le système d'exploitation et l'iDRAC.

Lorsque vous réactivez ces fonctionnalités de surveillance via les interfaces iDRAC ultérieurement, les mêmes vérifications sont effectuées et les fonctionnalités sont activées selon qu'OpenManage Server Administrator est en cours d'exécution ou non.

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 **Présentation générale** > **Serveur** > **Service Module**.
   La page **Configuration de l'iDRAC Service Module** s'affiche.
2. Vous pouvez afficher ce qui suit :
   - La version de l'iDRAC installée sur le système d'exploitation hôte
   - L'état de connexion de l'iDRAC Service Module à l'iDRAC.
3. Pour utiliser des fonctions de surveillance hors bande, sélectionnez une ou plusieurs des options suivantes :
   - **Informations sur le système d'exploitation** : affiche les informations sur le système d'exploitation.

- **Répliquer le journal Lifecycle dans le journal du système d'exploitation** : inclut les journaux Lifecycle Controller aux journaux du système d'exploitation. Cette option est désactivée si OpenManage Server Administrator est installé sur le système.
- **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) :
  - **Redémarrer**
  - **Arrêter le système**
  - **Exécuter un cycle d'alimentation sur le système**

  Cette option est désactivée si OpenManage Server Administrator est installé sur le système.

Utilisation 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 en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Utilisation d'iDRAC Service Module d'iDRAC sur Windows Nano

Pour des instructions d'installation, voir l'*iDRAC Service Module User's Guide* (Guide d'utilisation du module Service iDRAC).

Pour vérifier si le service iSM est en cours d'exécution, utilisez la cmdlet suivante :

```
Get-Service "iDRAC Service Module"
```

La requête WMI ou Windows PowerShell vous permet d'afficher les journaux Lifecycle répliqués :

```
GetCimInstance -Namespace root/cimv2 - className win32_NTLogEvent
```

Par défaut, les journaux sont disponibles sur **Observateur d'événements** > **Journaux des applications et des services** > **Système**.

20

Utilisation d'un port USB pour la gestion de serveur

Dans les serveurs Dell PowerEdge de 12e génération, tous les ports USB sont dédiés au serveur. Avec les serveurs de 13e génération, l'un des ports USB du panneau avant est utilisé par iDRAC à des fins de gestion telles que le pré-provisionnement et le dépannage. Le port possède une icône pour indiquer qu'il s'agit d'un port de gestion. Tous les serveurs de 13e génération avec écran LCD prennent en charge cette fonction. Ce port n'est pas disponible dans certaines versions des modèles 200 à 500 sans panneau LCD. Dans ces cas, il est préférable d'utiliser ces ports pour le système d'exploitation du serveur.

REMARQUE : Cette fonction n'est pas prise en charge sur les serveurs PowerEdge R930.

Si le port USB est utilisé par iDRAC :

- L'interface réseau USB permet d'utiliser des outils de gestion à distance hors bande à partir d'un appareil portable, tel qu'un ordinateur portable à l'aide d'un câble de type A/A USB connecté à iDRAC. L'iDRAC reçoit l'adresse IP (169.254.0.3) et l'ordinateur portable reçoit l'adresse IP 169.254.0.4.
- Vous pouvez stocker un profil de configuration de serveur dans le périphérique USB et mettre à jour la configuration du serveur à partir du périphérique USB.

REMARQUE : Cette fonctionnalité est prise en charge sur :

- Les périphériques USB dotés de système de fichiers FAT et disposant d'une seule partition.
- Toutes les tablettes Dell Windows 8 et Windows RT, y compris le XPS 10 et le Venue Pro 8. Pour les périphériques avec un mini port USB, tels que le XPS 10 et le Venue Pro 8, utilisez la clé OTG (On-The -Go) et un câble de type A/A.

Concepts associés

Configuration de l'iDRAC à l'aide du profil de configuration de serveur sur un périphérique USB , page 285

Tâches associées

Accès à l'interface iDRAC via connexion USB directe , page 284

Sujets :

- Accès à l'interface iDRAC via connexion USB directe
- Configuration de l'iDRAC à l'aide du profil de configuration de serveur sur un périphérique USB

Accès à l'interface iDRAC via connexion USB directe

La fonction iDRAC Direct permet la connexion directe de 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 WSMan pour une gestion et une maintenance de serveur avancées.

Utilisez un câble de type A/A pour connecter l'ordinateur portable au serveur.

Lorsque iDRAC se comporte comme un périphérique USB et que le mode du port de gestion est défini sur **Automatic (Automatique)**, iDRAC utilise toujours le port USB. Le port ne passe pas automatiquement au système d'exploitation.

Pour obtenir une liste des navigateurs et des systèmes d'exploitation pris en charge, consultez le fichier de Notes de mise à jour, disponible sur dell.com/idracmanuals.

REMARQUE : Si vous utilisez des systèmes d'exploitation Windows, il peut être nécessaire d'installer un pilote RNDIS pour pouvoir utiliser cette fonction.

Pour accéder à l'interface iDRAC via le port USB :

1. Mettez hors tension tous les réseaux sans fil et déconnectez-les de tout autre réseau filaire.
2. Vérifiez que le port USB est activé. Pour plus d'informations, voir Configuration des paramètres du port de gestion USB , page 285.

3. Connectez un câble de type A/A de l'ordinateur portable au port USB de l'iDRAC.
   Le voyant LED de gestion s'allume en vert et reste allumé pendant deux secondes.
4. Attendez que l'ordinateur portable et l'iDRAC obtiennent les adresses IP 169.254.0.4 et 169.254.0.3. L'acquisition des adresses IP peut prendre quelques secondes.
5. Commencez à utiliser les interfaces réseau iDRAC, comme l'interface Web, RACADM ou WSMan.
6. Lorsque l'iDRAC utilise le port USB, le voyant LED clignote pour indiquer la présence d'activité. Le voyant clignote quatre fois par seconde.
7. Une fois les actions souhaitées terminées, débranchez le câble USB du système.
   Le voyant LED s'éteint.

Configuration de l'iDRAC à l'aide du profil de configuration de serveur sur un périphérique USB

Avec la nouvelle fonction iDRAC Direct, vous pouvez configurer l'iDRAC au niveau du serveur. Commencez par configurer les paramètres de port de gestion USB sur 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 vers l'iDRAC.

REMARQUE : Vous pouvez définir les paramètres de port de gestion USB à l'aide des interfaces iDRAC uniquement si aucun périphérique USB n'est connecté au serveur.

REMARQUE : Les serveurs PowerEdge sans écran LCD ni panneau à voyants LED ne prennent pas en charge la clé USB.

Concepts associés

Configuration des paramètres du port de gestion USB , page 285

Tâches associées

Importation du profil de configuration de serveur depuis un périphérique USB , page 287

Configuration des paramètres du port de gestion USB

Vous pouvez configurer le port USB dans iDRAC :

- Activez ou désactivez le port USB d'un serveur à l'aide de la configuration du BIOS. Lorsque vous le réglez sur **Tous les ports désactivés** ou **Tous les ports à l'avant désactivés**, iDRAC désactive également le port USB géré. Vous pouvez afficher l'état du port à l'aide des interfaces iDRAC. Si l'état est Désactivé :
  - iDRAC ne traite pas de périphérique USB ou hôte connecté au port USB géré.
  - Vous pouvez modifier la configuration de l'USB géré, mais les paramètres n'entrent pas en vigueur avant l'activation des ports USB du panneau avant dans le BIOS.
- Définissez le Mode de port de gestion USB qui détermine si le port USB est utilisé par iDRAC ou le SE du serveur :
  - Automatique (par défaut) : si un périphérique USB n'est pas pris en charge par iDRAC ou si le profil de configuration du serveur n'est pas présent sur le périphérique, le port USB est déconnecté d'iDRAC et connecté au serveur. Lorsqu'un périphérique est supprimé du serveur, la configuration du port est réinitialisée et peut être utilisée par iDRAC.
  - Utilisation SE standard : le périphérique USB est toujours utilisé par le système d'exploitation.
  - iDRAC direct uniquement : le périphérique USB est toujours utilisé par iDRAC.

Vous devez disposer des privilèges de contrôle du serveur pour configurer le port de gestion 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 Automatique ou iDRAC et le périphérique USB est inséré ou retiré.
- Le Mode Port de gestion USB est modifié.
- Le périphérique est automatiquement transféré d'iDRAC au SE.
- Le périphérique est retiré d'iDRAC ou du SE

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 autorisés : e-mail, interruption SNMP, journal syslog distant et Événements WS en cours.
- Actions : Aucune.

Un message d'erreur s'affiche et est consigné dans le journal du Lifecycle Controller dans les cas suivants :

- Vous essayez de configurer le port de gestion USB sans le privilège de contrôle du serveur.
- Un périphérique USB est en cours d'utilisation par l'iDRAC et vous tentez de modifier le Mode Port de gestion USB.
- Un périphérique USB est en cours d'utilisation par l'iDRAC et vous retirez le périphérique.

Configuration du port de gestion USB à l'aide de l'interface Web

Pour configurer le port USB :

1. Dans l'interface Web iDRAC, allez sous **Présentation** > **Matériel** > **Port de gestion USB**.
   La page **Configuration du port de gestion USB** s'affiche.
2. Dans le menu déroulant **Mode de port de gestion USB**, sélectionnez l'une des options suivantes :
   - **Automatique** : le port USB est utilisé par iDRAC ou le système d'exploitation du serveur.
   - **Utilisation SE standard** : le port USB est utilisé par le SE du serveur.
   - **iDRAC direct uniquement** : le port USB est utilisé par iDRAC.
3. À partir de l'iDRAC géré : dans le menu déroulant Configuration XML USB, sélectionnez les options pour configurer un serveur en important des fichiers de configuration XML stockés sur un lecteur USB :
   - **Désactivée**
   - **Activé uniquement lorsque le serveur est doté de paramètres de références par défaut**
   - **Activée**

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
4. Cliquez sur **Appliquer** pour appliquer les paramètres.

Configuration du port de gestion USB à l'aide de RACADM

Pour configurer le port de gestion USB, utilisez les objets et sous-commandes RACADM :

- Pour afficher l'état du port USB :

```
racadm get iDRAC.USB.ManagementPortStatus
```

- Pour afficher la configuration du port USB :

```
racadm get iDRAC.USB.ManagementPortMode
```

- Pour modifier la configuration du port USB :

```
racadm set iDRAC.USB.ManagementPortMode <Automatic|Standard OS Use|iDRAC|>
```

REMARQUE : Assurez-vous de mettre l'attribut Standard OS Use (Utilisation SE standard) entre guillemets simples lors de l'utilisation de la commande set RACADM.

- Pour afficher l'inventaire des périphériques USB :

```
racadm hwinventory
```

- Pour configurer une nouvelle configuration d'alerte :

```
racadm eventfilters
```

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration du port de gestion USB à l'aide de l'utilitaire de configuration d'iDRAC

Pour configurer le port USB :

1. Dans l'utilitaire de configuration d'iDRAC, accédez à **Paramètres de port USB et de média**.
   La page **Paramètres de port USB et de média de configuration d'iDRAC** s'affiche.
2. Dans le menu déroulant **Mode de port de gestion USB**, procédez comme suit :
   - **Automatique** : le port USB est utilisé par iDRAC ou le système d'exploitation du serveur.
   - **Utilisation SE standard** : le port USB est utilisé par le SE du serveur.
   - **iDRAC direct uniquement** : le port USB est utilisé par iDRAC.
3. À partir du menu déroulant **iDRAC direct : fichier XML de configuration USB**, sélectionnez les options pour configurer un serveur en important un profil de configuration de serveur stocké sur un lecteur USB :
   - **Désactivée**
   - **Activé tant que le serveur dispose de paramètres de références par défaut uniquement**
   - **Activée**

   Pour plus d'informations sur les champs, voir l'*Aide en ligne de l'utilitaire de configuration d'iDRAC*.
4. Cliquez successivement sur **Retour**, **Terminer** et **Oui**. Les paramètres sont enregistrés.

Importation du profil de configuration de serveur depuis un périphérique USB

Veillez à créer, à la racine du périphérique USB, un répertoire appelé `System_Configuration_XML` qui contient les fichiers `config.xml` et `control.xml` :

- Le profil de configuration de serveur 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 d'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`, `<modelnumber>-config.xml` ou `config.xml`.
- Fichier XML de contrôle : comprend des paramètres de contrôle afin de contrôler l'opération d'importation et ne possède pas les attributs d'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/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 profil de configuration du serveur, la modification des paramètres de gestion de l'USB dans le fichier XML entraîne l'échec d'une tâche ou l'exécution d'une tâche avec des erreurs. Afin d'éviter les erreurs, vous pouvez indiquer que les attributs figurant dans le fichier XML doivent être ignorés.

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 **Automatique** ou **iDRAC**.

- Définissez **iDRAC géré : configuration XML 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.
3. Le profil de configuration de 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`
   - `<modelnum>-config.xml`
   - `config.xml`
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 XML 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. L'écran LCD et le voyant LED (le cas échéant) indiquent que le travail d'importation a démarré.
6. Si une configuration doit être préparée et le **Type d'arrêt** est défini sur **Ne pas redémarrer** dans le fichier de contrôle, vous devez redémarrer le serveur pour que les paramètres soient configurés. Sinon, le serveur est redémarré et la configuration est appliquée. C'est uniquement lorsque le serveur est déjà sous tension que la configuration préparée s'applique même si l'option **Ne pas redémarrer** est spécifiée.
7. Une fois l'importation terminée, le LCD/LED indique que la tâche est terminée. Si un redémarrage est nécessaire, l'écran LCD affiche l'état de la tâche comme « En suspend, en attente de redémarrage ».
8. Si le périphérique USB reste inséré sur le serveur, le résultat de l'opération d'importation est enregistré dans le fichier `results.xml` dans le périphérique USB.

Messages LCD

Si l'écran LCD est disponible, il affiche le message suivant dans une séquence :

1. Importation : lorsque le profil de configuration de serveur est copié du périphérique USB.
2. Application : lorsque la tâche est en cours.
3. Terminé : lorsque la tâche s'est terminée avec succès.
4. Terminé avec des erreurs : lorsque la tâche s'est terminée avec des erreurs.
5. Échec : lorsque le travail a échoué.

Pour obtenir plus de détails, consultez le fichier de résultats sur le périphérique USB.

Comportement du clignotement des voyants LED

Si le voyant USB est présent, il indique ce qui suit :

- Vert fixe : lorsque le profil de configuration de serveur est copié du périphérique USB.
- Vert clignotant : lorsque le travail est en cours.
- Vert fixe : lorsque la tâche s'est terminée avec succès.

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 :

- Numéro 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.

21

Utilisation de la fonction Quick Sync (Synchronisation rapide) d'iDRAC

Quelques serveurs Dell PowerEdge 13e génération disposent de la bordure Quick Sync qui prend en charge la fonction Quick Sync. Cette fonction permet une gestion au niveau du serveur à partir d'un appareil mobile. Vous pouvez ainsi accéder à l'inventaire et aux informations de surveillance et configurer les paramètres de base d'iDRAC (tels que la configuration des références root et la configuration du premier périphérique d'amorçage) à l'aide du périphérique mobile.

Vous pouvez configurer l'accès à la fonction Quick Sync d'iDRAC pour votre appareil mobile (par exemple, OpenManage Mobile) dans l'iDRAC. Vous devez installer l'application OpenManage Mobile sur le périphérique mobile pour gérer le serveur à l'aide de l'interface Quick Sync d'iDRAC.

REMARQUE : Cette fonctionnalité est actuellement prise en charge sur les périphériques mobiles dotés du système d'exploitation Android.

Dans la version actuelle, cette fonction est disponible uniquement avec les serveurs en rack Dell PowerEdge R730, R730xd et R630. Pour ces serveurs, vous pouvez acheter une bordure en option. Il s'agit donc d'un matériel de vente incitative et les capacités de la fonction ne dépendent pas des licences logicielles d'iDRAC.

La fonction Quick Sync d'iDRAC comprend les éléments suivants :

- Bouton d'activation : vous devez appuyer sur ce bouton pour activer l'interface Quick Sync. Dans une infrastructure en rack bien empilée, cela permet d'identifier et d'activer le serveur cible pour la communication. La fonction Quick Sync est désactivée après avoir été inactive pendant un intervalle de temps défini (la valeur par défaut est 30 secondes) ou lorsque vous appuyez dessus pour la désactiver.
- Voyant LED d'activité : si Quick Sync est désactivé, le voyant LED clignote quelques fois puis s'éteint. De plus, si le temporisateur d'inactivité configurable est déclenché, le voyant LED s'éteint et désactive l'interface.

Après avoir configuré les paramètres de la fonction Quick Sync d'iDRAC dans l'iDRAC, maintenez l'appareil mobile à moins de deux centimètres, et lisez des informations pertinentes sur le serveur et les paramètres de configuration d'iDRAC.

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, consultez le *OpenManage Mobile User's Guide (Guide d'utilisation d'OpenManage Mobile)* sur le site **dell.com/manuals**.

Concepts associés

Configuration de la fonction Quick Sync (Synchronisation rapide) d'iDRAC , page 289
Utilisation d'un appareil mobile pour afficher des informations sur iDRAC , page 291

Sujets :

- Configuration de la fonction Quick Sync (Synchronisation rapide) d'iDRAC
- Utilisation d'un appareil mobile pour afficher des informations sur iDRAC

Configuration de la fonction Quick Sync (Synchronisation rapide) d'iDRAC

À l'aide de l'interface Web iDRAC ou RACADM, vous pouvez configurer la fonction Quick Sync d'iDRAC pour autoriser l'accès au périphérique mobile :

- Accès : vous pouvez spécifier l'une des options suivantes pour configurer l'état d'accès de la fonction Quick Sync iDRAC :
  - Lecture-Écriture : état par défaut.

- Accès lecture/écriture : permet de configurer les paramètres de base de l'iDRAC.
- Accès en lecture seule : permet d'afficher l'inventaire et les données de surveillance.
- Accès désactivé : ne permet pas l'affichage des informations et des paramètres de configuration.

- Délai d'expiration : vous permet d'activer ou de désactiver le temporisateur d'inactivité Quick Sync de l'iDRAC :
  - Si cette option est activée, elle vous permet de spécifier une période à la fin de laquelle le mode Quick Sync est désactivé. Pour l'activer, appuyez à nouveau sur le bouton d'activation.
  - Si cette option est désactivée, l'horloge ne vous permet pas de spécifier une valeur d'expiration.
- Limite du délai d'expiration : vous permet d'indiquer la période à la fin de laquelle le mode Quick Sync est désactivé. La valeur par défaut est de 30 secondes.

Vous devez disposer des privilèges de contrôle du serveur pour configurer les paramètres. Un redémarrage du serveur n'est pas nécessaire pour que les paramètres entrent en vigueur.

Une entrée est consignée dans le journal du Lifecycle Controller lorsque la configuration est modifiée.

Configuration des paramètres de la fonction Quick Sync (Synchronisation rapide) d'iDRAC à l'aide de l'interface Web

Pour configurer Quick Sync d'iDRAC :

1. Dans l'interface Web iDRAC, allez à**Présentation** > **Matériel** > **Panneau avant**.
2. Dans la section **Quick Sync iDRAC**, dans le menu déroulant **Accès**, sélectionnez une des options suivantes pour fournir un accès à l'appareil mobile Android :
   - Lecture/écriture
   - Lecture seule
   - Désactivée
3. Activez le temporisateur.
4. Spécifiez la valeur du délai d'attente.

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'iDRAC*.
5. Cliquez sur **Appliquer** pour appliquer les paramètres.

Configuration des paramètres de la fonction Quick Sync (Synchronisation rapide) d'iDRAC à l'aide de RACADM

Pour configurer la fonction Quick Sync (Synchronisation rapide) d'iDRAC, utilisez les objets racadm du groupe **System.QuickSync**. Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Configuration des paramètres de la fonction Quick Sync (Synchronisation rapide) d'iDRAC à l'aide de l'utilitaire de configuration d'iDRAC

Pour configurer iDRAC Quick Sync d'iDRAC :

1. Dans l'utilitaire de configuration d'iDRAC, allez sous **Sécurité du panneau avant**.
   La page **Sécurité du panneau avant des paramètres iDRAC** s'affiche.
2. Dans la section **Quick Sync iDRAC** :
   - Spécifiez le niveau d'accès.
   - Activez le délai.
   - Spécifiez la Limite du délai défini par l'utilisateur (15 secondes à 3 600 secondes).

   Pour plus d'informations sur les champs, voir l'*Aide en ligne d'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 les informations de l'iDRAC depuis l'appareil mobile, voir le *OpenManage Mobile User's Guide* (Guide d'utilisation d'OpenManage Mobile) disponible à l'adresse **dell.com/support/manuals** .

22

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
- Console Média Virtuel

Tâches associées

Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance , page 292
Déploiement d'un système d'exploitation à l'aide de Média Virtuel , page 294

Sujets :

- Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance
- Déploiement d'un système d'exploitation à l'aide de Média Virtuel
- Déploiement d'un système d'exploitation intégré sur une carte SD

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 de réseau contient des pilotes et un fichier d'image amorçable du système d'exploitation dans un format standard, tel que **.img** ou **.iso**.

  REMARQUE : Lors de la création du fichier image, suivez les procédures d'installation réseau standard et marquez l'image de déploiement comme étant en lecture seule pour que chaque système cible démarre et exécute la même procédure de déploiement.

Pour déployer un système d'exploitation à l'aide de RFS :

1. À l'aide de RFS, montez le fichier d'image ISO ou IMG sur le système géré par l'intermédiaire de NFS, CIFS, HTTP ou HTTPS.
2. Accédez à **Présentation** > **Configuration** > **Premier périphérique de démarrage**.
3. Définissez la séquence de démarrage dans la liste déroulante **Premier périphérique de démarrage** pour sélectionner un support virtuel tel qu'une disquette, un CD, un DVD ou ISO.
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.

Concepts associés

Gestion du partage de fichier à distance , page 292
Définition du premier périphérique de démarrage , page 92

Gestion du partage de fichier à distance

Avec la fonction de partage de fichier à distance (RFS), vous pouvez définir un fichier image ISO ou IMG situé sur un partage de réseau et le rendre accessible au système d'exploitation du serveur géré comme lecteur virtuel en le montant comme CD ou DVD à l'aide de NFS, CIFS, HTTP ou HTTPS. Cette fonction est disponible sous licence.

REMARQUE : CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.

Le partage de fichiers à distance ne prend en charge que les formats de fichier d'image **.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.

REMARQUE : Si ESXi fonctionne sur un système géré et que vous montez une image de disquette (**.img**) en utilisant le partage de fichier à distance, l'image de disquette virtuelle n'est pas accessible au système d'exploitation ESXi.

RFS et les fonctionnalités de média virtuel sont mutuellement exclusifs.

- Si le client média virtuel n'a pas été lancé, et que vous tentez d'établir une connexion RFS, celle-ci est établie et l'image distante devient accessible au système d'exploitation hôte.
- Si le client média virtuel a été lancé et que vous tentez d'établir une connexion RFS, le message d'erreur suivant s'affiche :

  Le Média virtuel est détaché ou redirigé pour le lecteur virtuel sélectionné.

L'état de connexion RFS est disponible dans le journal iDRAC. Une fois connecté, un lecteur virtuel monté avec RFS ne se déconnecte pas, même si vous fermez la session dans iDRAC. La connexion RFS est fermée si l'iDRAC est réinitialisé ou si la connexion réseau est perdue. L'interface Web et les options de ligne de commande sont également disponibles dans le CMC et l'iDRAC pour fermer la connexion RFS. La connexion RFS depuis le CMC remplace toujours un montage RFS existant dans iDRAC.

REMARQUE : La fonction vFlash iDRAC et RFS ne sont pas associées.

Si vous mettez à jour le micrologiciel iDRAC de la version 1.30.30 à 1.50.50 alors qu'il existe une connexion RFS active et que le mode de connexion du média virtuel est défini sur **Connecter** ou **Auto-connecter**, l'iDRAC tente de rétablir la connexion RFS après la mise à niveau du micrologiciel et le redémarrage de l'iDRAC.

Si vous mettez à jour le micrologiciel iDRAC de la version 1.30.30 à 1.50.50 alors qu'il existe une connexion RFS active et que le mode de connexion du média virtuel est défini sur **Déconnecter**, l'iDRAC ne tente pas de rétablir la connexion RFS après la mise à niveau du micrologiciel et le redémarrage de l'iDRAC.

Configuration du partage de fichier à distance à l'aide de l'interface web

Pour activer le partage de fichier à distance :

1. Dans l'interface Web d'iDRAC, accédez à **Présentation** > **Serveur** > **Média connecté**.
   La page **Média connecté** s'affiche.
2. Sous **Médias connectés**, sélectionnez **Connecter** ou **Connecter automatiquement**.
3. Sous **Partage de fichier à distance**, 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 : //<adresse IP pour connexion au système de fichiers CIFS>/<chemin de fichier>/<nom de l'image>
   - NFS : <adresse IP pour connexion au système de fichiers NFS>:/<chemin de fichier>/<nom de l'image>
   - HTTP : http://<URL>/<chemin d'accès au fichier>/<nom de l'image>
   - HTTPS : https://<URL>/<chemin d'accès au fichier>/<nom de l'image>

   REMARQUE : CIFS prend en charge à la fois les adresses IPv4 et IPv6, mais NFS ne prend en charge que l'adresse IPv4.

   REMARQUE : Les caractères '/' ou '\' peuvent être utilisés pour le chemin d'accès au fichier.

   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, voir Caractères recommandés pour les noms d'utilisateur et mots de passe , page 133.

   REMARQUE : Lorsque vous indiquez les paramètres de partage du 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.

4. Cliquez sur **Appliquer**, puis sur **Connecter**.
   Une fois la connexion établie, l'**État de la connexion** indique **Connecté**.

REMARQUE : Même si vous avez configuré le partage de fichier à distance, l'interface utilisateur n'affiche pas les informations d'identification de l'utilisateur pour des raisons de sécurité.

Pour les distributions Linux, cette fonction peut nécessiter une commande de montage manuel au niveau d'exécution init 3. La syntaxe de la commande est :

```
mount /dev/OS_specific_device / user_defined_mount_point
```

où, `user_defined_mount_point` correspond à un répertoire que vous choisissez d'utiliser comme pour n'importe quelle commande de montage.

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

Pour SLES, le périphérique 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 une image

`-d` : déconnecter une image

`-u` <nom d'utilisateur> : nom d'utilisateur permettant d'accéder au partage de réseau

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

`-l` <image_emplacement>: emplacement de l'image sur le partage réseau ; utilisez des guillemets doubles autour du nom de l'emplacement. Voir des exemples de chemin de fichier d'image dans la section Configuration du partage de fichiers à distance à l'aide de l'interface Web

`-s` : affiche l'état actuel

REMARQUE : Tous les caractères, notamment les caractères alphanumériques et spéciaux, peuvent figurer dans le nom d'utilisateur, le mot de passe et l'emplacement de l'image, à l'exception des caractères suivants : ' (guillemet simple), " (guillemets doubles), , (virgule), < (inférieur à) et > (supérieur à).

Déploiement d'un système d'exploitation à l'aide de Média Virtuel

Avant de déployer un système d'exploitation à l'aide de Média Virtuel, vérifiez que :

- Média Virtuel est *connecté* pour que les lecteurs virtuels apparaissent dans la séquence de démarrage.
- Si Média Virtuel fonctionne en mode de *connexion automatique*, l'application Média Virtuel doit être lancée avant le démarrage du système.
- Le partage de réseau contient 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.

Concepts associés

Configuration de média virtuel , page 248
Définition du premier périphérique de démarrage , page 92

Tâches associées

Configuration de l'iDRAC , page 81

Installation d'un système d'exploitation depuis plusieurs disques

1. Dissociez le CD/DVD existant.
2. Insérez le CD/DVD suivant dans le lecteur optique distant.
3. Associez de nouveau le lecteur de CD/DVD.

Déploiement d'un système d'exploitation intégré sur une carte SD

Pour installer un hyperviseur intégré sur une carte SD :

1. Insérez les deux cartes SD dans les logements IDSDM (Internal Dual SD Module) sur le système.
2. Activez le module et la redondance SD (si nécessaire) dans le BIOS.
3. Vérifiez que la carte SD est disponible sur l'un des lecteurs lorsque vous appuyez sur <F11> lors du démarrage.
4. Déployez le système d'exploitation intégré et suivez les instructions d'installation.

Concepts associés

À propos d'IDSDM , page 296

Tâches associées

Activation du module SD et de la redondance dans le BIOS , page 295

Activation du module SD et de la redondance dans le BIOS

Pour activer le module SD et la redondance dans le BIOS :

1. Appuyez sur <F2> lors du démarrage.
2. Accédez à **Configuration du système** > **Paramètres du BIOS du système** > **Périphériques intégrés**.
3. Affectez à **Port USB interne** la valeur **Actif**. Si la valeur est **Inactif**, IDSDM n'est pas disponible comme périphérique de démarrage.
4. Si la redondance n'est pas nécessaire (carte SD unique), affectez à **Port de carte SD interne** la valeur **Actif** et à **Redondance de carte SD interne** la valeur **Désactivé**.
5. Si la redondance est nécessaire (deux cartes SD), affectez à **Port de carte SD interne** la valeur **Actif** et à **Redondance de carte SD interne** la valeur **Miroir**.
6. Cliquez sur **Retour**, puis sur **Terminer**.

7. Cliquez sur **Oui** pour enregistrer les paramètres et appuyez sur <Échap> pour quitter le programme de **Configuration du système**.

À propos d'IDSDM

Le module IDSDM (Internal Dual SD Module) est disponible uniquement sur les plates-formes applicables. IDSDM fournit une redondance sur la carte SD de l'hyperviseur en utilisant une autre carte SD qui met en miroir le contenu de la première carte SD.

L'une ou l'autre des cartes SD peut être la carte principale. Par exemple, si deux nouvelles cartes SD sont installées dans le module IDSDM, SD1 est active (carte principale) et SD2 est la carte de secours. Les données sont écrites sur les deux cartes, mais elles sont lues sur SD1. Si la carte SD1 est défaillante ou supprimée, SD2 devient automatiquement la carte active (carte principale).

Vous pouvez afficher l'état, l'intégrité et la disponibilité d'IDSDM à l'aide de l'interface Web iDRAC ou RACADM. L'état de redondance et les événements d'erreur de la carte SD sont journalisés dans le journal SEL affiché sur le panneau avant, et des alertes PET sont générées si les alertes sont activées.

Concepts associés

Affichage des informations des capteurs , page 107

23

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 ;
- Intégrité du système.

Tâches associées

Utilisation de la console de diagnostic , page 297
Planification de diagnostics automatisés à distance , page 298
Affichage des codes du Post , page 299
Affichage des vidéos de capture de démarrage et de blocage , page 299
Affichage des journaux , page 299
Affichage de l'écran du dernier blocage du système , page 300
Affichage de l'état du panneau avant , page 300
Voyants des problèmes matériels , page 301
Affichage de l'intégrité du système , page 301
Génération de la collecte SupportAssist , page 302

Sujets :

- Utilisation de la console de diagnostic
- Affichage des codes du Post
- Affichage des vidéos de capture de démarrage et de blocage
- Affichage des journaux
- Affichage de l'écran du dernier blocage du système
- Affichage de l'état du panneau avant
- Voyants des problèmes matériels
- Affichage de l'intégrité du système
- Génération de la collecte SupportAssist
- Vérification des messages d'erreur dans l'écran d'état du serveur
- Redémarrage d'iDRAC
- Effacement des données système et utilisateur
- Restauration des paramètres par défaut définis en usine d'iDRAC

Utilisation de la console de diagnostic

iDRAC fournit un ensemble d'outils standard de diagnostic réseau similaires aux outils des systèmes Microsoft Windows et Linux. En utilisant l'interface Web iDRAC, vous pouvez accéder aux outils de débogage réseau.

Pour accéder à la console de diagnostic :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Dépannage** > **Diagnostics**.
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 d'iDRAC*.
   Les résultats s'affichent sur la même page.

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 pouvez également exécuter des diagnostics en utilisant la ou les commandes WSMAN appropriées. Pour plus d'informations, voir la documentation de WSMAN.

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 WSMAN ou 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 à l'aide de RACADM

- Pour exécuter les diagnostics à distance et enregistrer les résultats sur le système local, utilisez la commande suivante :

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
```

- Pour exporter les résultats de la dernière exécution de tests de diagnostic à distance, utilisez la commande suivante :

```
racadm diagnostics export -f <file name> -l <NFS / CIFS / HTTP / HTTPS share> -u
<username> -p <password>
```

Pour plus d'informations sur ces options, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Affichage des codes du Post

Les codes Post sont des indicateurs d'avancement du BIOS du système, qui indiquent les étapes de la séquence de démarrage depuis une réinitialisation avec mise sous tension. Ils permettent d'identifier les problèmes liés au démarrage du système. La page **Codes du Post** affiche le dernier code Post système avant le démarrage du système.

Pour afficher les codes du Post, accédez à **Présentation générale** > **Serveur** > **Dépannage** > **Code du Post**.

La page **Code du POST** affiche l'indicateur d'intégrité du système, un code hexadécimal et la description du code.

Affichage des vidéos de capture de démarrage et de blocage

Vous pouvez afficher les vidéos de :

- Trois derniers cycles de démarrage : une vidéo de cycle de démarrage enregistre la séquence des événements d'un cycle de démarrage. Les vidéos de cycle de démarrage sont organisées du dernier démarrage au premier démarrage.
- Vidéo du dernier blocage : une vidéo de blocage enregistre la séquence d'événements précédant le blocage.

Il s'agit d'une fonction sous licence.

iDRAC enregistre cinquante trames au cours du démarrage. La lecture des écrans de démarrage s'effectue à raison d'une trame par seconde. Si iDRAC est réinitialisé, la vidéo de capture de démarrage n'est pas disponible, car elle est stockée en mémoire RAM et supprimée.

REMARQUE :

- Vous devez disposer des privilèges d'accès à la console virtuelle ou Administrateur pour lire les vidéo de capture de démarrage et de blocage.
- L'heure de capture de la vidéo affichée dans le lecteur vidéo de l'interface utilisateur graphique iDRAC peut différer de celle affichée dans d'autres lecteurs vidéo. Le lecteur vidéo iDRAC affiche en effet l'heure dans le fuseau horaire d'iDRAC alors que tous les autres lecteurs vidéo l'affichent dans l'heure de leurs systèmes d'exploitation respectifs.

Pour afficher l'écran de **Capture du démarrage**, cliquez sur **Présentation** > **Serveur** > **Dépannage** > **Capture vidéo**.

L'écran **Capture vidéo** affiche les enregistrements vidéo. Pour en savoir plus, voir l'*aide en ligne d'iDRAC*.

Configuration des paramètres de capture vidéo

Pour configurer les paramètres de capture vidéo :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **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 d'amorçage 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 d'amorçage 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 SEL (System Event Logs) et les journaux Lifecycle. Pour plus d'informations, voir Affichage du journal des événements système et Affichage du journal Lifecycle .

Affichage de l'écran du dernier blocage du système

La fonction d'écran du dernier blocage crée une capture d'écran du dernier blocage du système, l'enregistre et l'affiche dans iDRAC. Cette fonction est disponible sous licence.

Pour afficher l'écran du dernier blocage :

1. Vérifiez que la fonction d'écran du dernier blocage système est activée.
2. Dans l'interface Web 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.

Concepts associés

Activation du dernier écran de blocage , page 93

Affichage de l'état du panneau avant

Le panneau avant du système géré résume l'état des composants suivants du système :

- Batteries
- Ventilateurs
- Intrusion
- Blocs d'alimentation
- Média flash amovible
- Températures
- Tensions

Vous pouvez afficher l'état du panneau avant du système géré :

- Pour les serveurs en rack et de type tour : état du panneau avant LCD et du voyant LED d'ID système ou état du panneau avant LED et voyant d'ID système.
- Pour les serveurs lames : uniquement les voyants d'ID système.

Affichage de l’état du panneau avant LCD

Pour afficher l’état du panneau avant LCD des serveurs en rack et de type tour applicables, dans l’interface Web iDRAC, accédez à **Overview (Présentation)** > **Hardware (Matériel)** > **Front Panel (Panneau avant)**. La page **Front Panel (Panneau avant)** s’affiche.

La section **Live Front Panel Feed (Flux en direct du panneau avant)** affiche les messages actuellement affichés sur le panneau avant LCD. Lorsque le système fonctionne normalement (voyant bleu fixe sur le panneau avant de l’écran LCD), **Hide Error (Masquer l’erreur)** et **UnHide Error (Afficher l’erreur)** sont grisés.

REMARQUE : Vous pouvez masquer ou afficher les erreurs uniquement pour les serveurs rack et de type tour.

Pour afficher l’état du panneau avant LCD à l’aide de RACADM, utilisez les objets du groupe `System.LCD`. Pour en savoir plus, voir le *Guide de référence de l’interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Concepts associés

Configuration du paramétrage LCD , page 90

Affichage de l’état LED du panneau avant du système

Pour afficher l’état LED d’ID système actuel, dans l’interface web d’iDRAC, accédez à **Présentation** > **Matériel** > **Panneau avant**. La section **Données dynamiques du panneau avant** affiche l’état actuel du panneau avant :

- Bleu fixe : aucune erreur sur le système géré.
- Bleu clignotant : le mode d’identification est activé (qu’il existe une erreur ou non sur le système géré).
- Orange fixe : le système géré est en mode Failsafe.

- Orange clignotant : erreur sur le système géré.

Lorsque le système fonctionne normalement (indiqué par une icône d'intégrité bleue dans les LED du panneau avant), **Masquer l'erreur** et **Afficher l'erreur** sont grisés. Vous pouvez afficher ou masquer les erreurs uniquement pour les serveurs en rack et de type tour.

Pour afficher l'état du LED d'ID système en utilisant l'interface RACADM, utilisez la commande `getled`.

Pour en savoir plus, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Concepts associés

Configuration du paramétrage LED d'ID système , page 91

Voyants des problèmes matériels

Les problèmes matériels sont les suivants :
- Défaillance de la mise sous tension
- Ventilateurs bruyants
- Perte de connectivité réseau
- Défaillance du disque dur
- Défaillance du média USB
- Endommagement physique

En fonction du problème, utilisez les méthodes suivantes pour éliminer le problème :
- Remettez le module ou le composant en place et redémarrez le système.
- S'il s'agit d'un serveur lame, insérez le module dans une autre baie dans le châssis.
- Remplacez les disques durs ou les lecteurs Flash USB
- Reconnectez ou remplacez les câbles d'alimentation et les câbles réseau

Si le problème persiste, voir le *Manuel du propriétaire du matériel* pour les informations de dépannage sur le périphérique matériel.

PRÉCAUTION : Vous devez exécuter les opérations de dépannage et de réparation simples indiquées dans la documentation du produit ou conformément aux instructions du service de maintenance téléphonique et du support technique. Les endommagements résultant d'opérations de maintenance non autorisées par Dell ne sont pas couverts par la garantie. Lisez et suivez les instructions de sécurité fournies avec le produit.

Affichage de l'intégrité du système

Les interfaces iDRAC et CMC (pour les serveurs lames) affichent l'état des éléments suivants :
- Batteries
- État du contrôleur de châssis
- Ventilateurs
- Intrusion
- Blocs d'alimentation
- Média flash amovible
- Températures
- Tensions
- UC

Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Récapitulatif du système** > **Intégrité du système**.

Pour afficher l'intégrité de l'UC, accédez à **Présentation** > **Matériel** > **UC**.

Les voyants d'intégrité du système sont les suivants :
- — Indique un état normal.
- — Indique un état d'avertissement.
- — Indique un état de défaillance.

- — Indique un état inconnu

Cliquez sur un nom de composant dans la section **Intégrité du serveur** pour afficher des informations sur le composant.

Génération de la collecte SupportAssist

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 envoyer les données à partir d'un autre système pour être certain que les données collectées à partir de votre serveur ne sont pas visibles par des individus non agréés lors de la transmission au support technique.

Vous pouvez générer un rapport d'intégrité du serveur, puis exporter le rapport vers un emplacement sur la station de gestion (locale) ou vers un emplacement de réseau partagé tel que le système de fichiers Internet commun (CIFS) ou le partage de fichiers réseau (NFS). Vous pouvez ensuite partager ce rapport directement avec le support technique. Pour exporter vers un partage réseau tel que CIFS ou NFS, la connectivité réseau directe au port réseau iDRAC partagé ou dédié est requise.

Le rapport est généré au format ZIP standard. Le rapport contient des informations similaires à celles disponibles dans le rapport DSET telles que :

- Matériel et inventaire de tous les composants
- Attributs des système, Lifecycle Controller et composants
- Informations sur le système d'exploitation et l'application
- Journaux du Lifecycle Controller actifs
- Journaux du Lifecycle Controller archivés
- Journaux de SSD PCIe
- Journaux du contrôleur de stockage

REMARQUE : La collecte TTYLog pour les disques SSD PCIe à l'aide de la fonction SupportAssist n'est pas prise en charge par les serveurs Dell PowerEdge de 12e génération.

Une fois les données générées, vous pouvez les afficher. Elles contiennent de nombreux fichiers XML et journaux. Les données doivent être partagées avec le support technique pour résoudre le problème.

Chaque fois que les données sont collectées, un événement est enregistré dans le journal du Lifecycle Controller. L'événement comprend des informations telles que l'interface utilisée, la date et l'heure de l'exportation et le nom d'utilisateur iDRAC.

Vous pouvez générer le rapport d'applications OS et des journaux de deux façons :

- Automatique : utilisation du Service module d'iDRAC qui appelle automatiquement l'outil OS Collector.
- Manuel : exécution manuelle du fichier exécutable de l'outil OS Collector depuis le système d'exploitation du serveur. L'iDRAC expose le fichier exécutable de l'outil OS Collector au système d'exploitation du serveur en tant que périphérique USB avec l'étiquette DRACRW.

REMARQUE :

- L'outil OS Collector ne s'applique pas aux systèmes Dell Precision PR7910.
- La fonction de collecte des journaux de l'OS n'est pas prise en charge sur le système d'exploitation CentOS.
- Dans les serveurs exécutant Windows 2016 Nano, le journal de l'afficheur HardwareEvent.evtx n'est pas généré par l'outil OS Collector. Pour générer le journal de l'afficheur HardwareEvent.evtx, exécutez la commande ~New-Item -Path HKLM:\SYSTEM\ControlSet001\Services\EventLog\HardwareEvents~ avant d'exécuter l'outil OS Collector.

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.

Concepts associés

Génération automatique de la collecte pour SupportAssist , page 303
Génération manuelle de la collecte SupportAssist , page 303

Génération automatique de la collecte pour SupportAssist

Si le module Service iDRAC est installé et en cours d'exécution, vous pouvez générer automatiquement la collecte de SupportAssist. L'iDRAC Service Module appelle le fichier de collecte approprié du SE sur le système d'exploitation hôte, collecte les données et les transfert à l'iDRAC. Vous pouvez ensuite enregistrer la collecte à l'emplacement requis.

Génération automatique de la collecte pour SupportAssist à l'aide de l'interface Web d'iDRAC

Pour générer automatiquement la collecte pour SupportAssist :

1. Dans l'interface web iDRAC, allez à **Présentation générale** > **Serveur** > **Dépannage** > **SupportAssist**.
   La page **SupportAssist** s'affiche.
2. Pour modifier les options de collecte de données, cliquez sur **Modifier les données de la collecte** :
   - **Matériel** : exportez la collecte SupportAssist du matériel.
   - **Journal du contrôleur RAID** : exportez la collecte SupportAssist du contrôleur RAID.
   - **Données du système d'exploitation et d'applications** : exportez la collecte SupportAssist des données du système d'exploitation et d'applications. Sous cette option, sélectionnez l'un des éléments suivants :
     - **Données standard** : sélectionnez cette option pour obtenir la collecte au format standard.
     - **Données filtrées** : sélectionnez cette option pour obtenir la collecte avec des données filtrées.

   REMARQUE : Par défaut, Matériel et système d'exploitation, ainsi que Données d'applications sont sélectionnés.
3. Sélectionnez l'option **J'ai lu et j'accepte les conditions générales**, puis cliquez sur **Continuer**.
4. Une fois que l'iDRAC Service Module a fini de transférer les données d'application et du SE vers iDRAC, celles-ci sont livrées avec les données du matériel et le rapport final est généré. Un message s'affiche pour enregistrer le rapport.
5. Spécifiez l'emplacement d'enregistrement de la collecte pour SupportAssist.

Génération manuelle de la collecte SupportAssist

Lorsqu'iSM n'est pas installé, vous pouvez exécuter manuellement l'outil OS Collector pour générer la collecte SupportAssist. Vous devez exécuter l'outil OS Collector sur le système d'exploitation du serveur afin d'exporter les données du système d'exploitation et des applications. Un périphérique USB virtuel intitulé DRACRW apparaît dans le système d'exploitation du serveur. Ce périphérique contient le fichier de l'outil OS Collector spécifique au système d'exploitation hôte. Exécutez le fichier spécifique au système d'exploitation à partir du système d'exploitation du serveur pour collecter et transférer les données vers l'iDRAC. Vous pouvez alors exporter les données vers un emplacement réseau local ou partagé.

Dans les serveurs Dell PowerEdge de 13e génération, le DUP de l'outil OS Collector est installé en usine. Toutefois, si vous estimez que l'OS Collector n'est pas présent dans l'iDRAC, vous pouvez télécharger le fichier DUP à partir du site de support de Dell, puis téléverser le fichier vers l'iDRAC à l'aide du processus de mise à jour du micrologiciel.

Avant de générer manuellement la collecte pour SupportAssist à l'aide de l'outil OS Collector, procédez comme suit sur le système d'exploitation hôte :

- Sur un système d'exploitation Linux : vérifiez si le service IPMI est en cours d'exécution. Si ce n'est pas le cas, vous devez démarrer le service manuellement. Le tableau suivant présente les commandes que vous pouvez utiliser pour vérifier l'état du service IPMI et démarrer le service (si nécessaire) pour chaque système d'exploitation Linux.

Tableau 47. Système d'exploitation Linux et commande de vérification du service IPMI

Sous LINUX	Commande pour vérifier l'état du service IPMI	Commande pour démarrer le service IPMI
Red Hat Enterprise Linux 5 64 bits Red Hat Enterprise Linux 6 SUSE Linux Enterprise Server 11 CentOS 6 Oracle VM Oracle Linux 6.4	`$ service ipmi status`	`$ service ipmi start`

Tableau 47. Système d'exploitation Linux et commande de vérification du service IPMI (suite)

Sous LINUX	Commande pour vérifier l'état du service IPMI	Commande pour démarrer le service IPMI
Red Hat Enterprise Linux 7	`$ systemctl status ipmi.service`	`$ systemctl start ipmi.service`

REMARQUE :
- CentOS est pris en charge uniquement pour l'iDRAC Service Module 2.0 ou version ultérieure.
- Si les modules IPMI ne sont pas présents, vous pouvez installer les modules respectifs à partir du support de distribution du SE. Le service démarre une fois l'installation terminée.

- Sous Windows :
  - Vérifiez que le service WMI est en cours d'exécution :
    - Si WMI est arrêté, l'OS Collector démarre le WMI automatiquement et poursuit la collection.
    - Si WMI est désactivé, la collecte de l'OS Collector s'arrête et affiche un message d'erreur.
  - Vérifiez les niveaux de privilèges appropriés et assurez-vous qu'aucun paramètre de pare-feu ou de sécurité ne vous empêche d'obtenir les données du registre ou du logiciel.

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 iDRAC, allez à **Présentation générale** > **Serveur** > **Dépannage** > **SupportAssist**.
   La page **SupportAssist** s'affiche.
2. Pour modifier les options de collecte de données, cliquez sur **Modifier les données de la collecte** :
   - **Matériel** : exportez la collecte SupportAssist du matériel.
   - **Journal du contrôleur RAID** : exportez la collecte SupportAssist du contrôleur RAID.
   - **Données du système d'exploitation et d'applications** : exportez la collecte SupportAssist des données du système d'exploitation et d'applications. Sous cette option, sélectionnez l'un des éléments suivants :
     - **Données standard** : sélectionnez cette option pour obtenir la collecte au format standard.
     - **Données filtrées** : sélectionnez cette option pour obtenir la collecte avec des données filtrées.

   REMARQUE : Par défaut, Matériel et système d'exploitation, ainsi que Données d'applications sont sélectionnés.

   Selon les options choisies, le temps nécessaire pour rassembler les données s'affiche en regard de ces options.

   Si l'outil OS Collector n'a pas été exécuté sur le système, l'option Données de système d'exploitation et d'applications est grisée et n'est pas sélectionnable. Le message Données de système d'exploitation et d'applications (horodatage : jamais) s'affiche.

   Si OS Collector a été exécuté sur le système par le passé, alors l'horodatage s'affiche lors de la collecte la plus récente des données du système d'exploitation et d'applications : Last Collected: <timestamp>

3. Cliquez sur **Connecter un OS Collector**.
   Vous êtes redirigé pour accéder au SE hôte. Un message qui vous invite à lancer la console virtuelle s'affiche.
4. Après le lancement de la console virtuelle, cliquez sur le message contextuel pour exécuter et utiliser l'outil OS Collecter pour collecter les données.
5. Accédez au périphérique USB virtuel DRACRW qui est présenté au système par l'iDRAC.
6. Appelez le fichier OS Collector approprié pour le système d'exploitation hôte :
   - Pour Windows, lancez **Windows_OSCollector_Startup.bat**.
   - Pour Linux, exécutez **Linux_OSCollector_Startup.exe**.
7. Une fois que l'OS Collector a terminé le transfert de données vers iDRAC, le périphérique USB est retiré automatiquement par iDRAC.
8. Retournez à la page **SupportAssist** et cliquez sur l'icône **Actualiser** pour refléter le nouvel horodatage.
9. Pour exporter les données, sous **Emplacement de l'exportation**, sélectionnez **Local** ou **Réseau**.
10. Si vous avez sélectionné l'option **Réseau**, entrez les détails relatifs à l'emplacement réseau.
11. Sélectionnez l'option **J'ai lu et j'accepte les conditions générales**, puis cliquez sur **Continuer**.

Génération manuelle de la collecte pour SupportAssist à l'aide de RACADM

Pour générer la collecte SupportAssist à l'aide de RACADM, utilisez la sous-commande **techsupreport**. Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Vérification des messages d'erreur dans l'écran d'état du serveur

Lorsqu'un voyant orange clignote et qu'un serveur est défaillant, l'écran principal d'état du serveur sur l'écran LCD indique en orange le serveur affecté. Utilisez les boutons de navigation de l'écran LCD pour sélectionner le serveur concerné, puis cliquez sur le bouton du milieu. Les messages d'erreur et d'avertissement s'affichent sur la deuxième ligne. Pour la liste des messages d'erreur affichés sur l'écran LCD, voir le manuel du propriétaire du serveur.

Redémarrage d'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 Web iDRAC

Vous pouvez redémarrer l'iDRAC à l'aide de l'une des méthodes suivantes : Une opération normale de redémarrage est réalisée sur l'iDRAC. Après le redémarrage, actualisez le navigateur pour vous reconnecter à l'iDRAC.

- Accédez à **Présentation** > **Serveur** > **Résumé**. Dans **Tâches de lancement rapide**, cliquez sur **Réinitialiser l'iDRAC**.
- Allez à **Présentation** > **Serveur** > **Dépannage** > **Diagnostics**. Cliquez sur **Réinitialiser l'iDRAC**.

Réinitialisation d'iDRAC à l'aide de l'interface RACADM

Pour redémarrer iDRAC, utilisez la commande **racreset**. Pour en savoir plus, voir le *RACADM Reference Guide for iDRAC and CMC* (Guide de référence RACADM d'iDRAC et de CMC) disponible à l'adresse **dell.com/support/manuals**.

Effacement des données système et utilisateur

Vous pouvez effacer des composants du système et des données utilisateur pour ces composants. Les composants du système sont les suivants :

- Données du Lifecycle Controller
- Diagnostics intégrés
- Pack de pilotes intégrés de l'OS
- Restauration des valeurs par défaut du BIOS
- Restauration des valeurs par défaut d'iDRAC

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 micrologiciel 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 de l'OS
- LCDATA : effacer les données du Lifecycle Controller
- IDRAC : restauration des valeurs par défaut d'iDRAC

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

REMARQUE : Le lien vers le Dell Tech Center apparaît dans l'interface GUI de l'iDRAC sur les systèmes de marque Dell. Si vous effacez les données du système à l'aide de la commande WSMan et que vous souhaitez que le lien s'affiche de nouveau, redémarrez l'hôte manuellement et attendez que CSIOR s'exécute.

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. Allez à **Présentation** > **Serveur** > **Dépannage** > **Diagnostics**.
   La page **Diagnostics de la console** s'affiche.
2. Cliquez sur **Réinitialiser iDRAC sur les paramètres par défaut**.
   L'état d'avancement s'affiche en pourcentage. L'iDRAC redémarre et est restauré sur ses paramètres par défaut. L'adresse IP d'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. Redémarrez le serveur et appuyez sur <F2>.
   La page de configuration du système s'affiche.
2. Cliquez sur **iDRAC Settings** (Paramètres iDRAC).
   La page de l'utilitaire Paramètres de l'iDRAC s'affiche.
3. Cliquez sur **Rétablir les valeurs par défaut de la configuration d'iDRAC**.
   La page **Paramètres iDRAC - Restauration des configurations par défaut iDRAC** s'affiche.
4. Cliquez sur **Oui**.
   La réinitialisation iDRAC démarre.
5. Cliquez sur **Retour** et accédez à la même page **Restauration des configurations par défaut iDRAC** pour afficher le message d'aboutissement.

24

Questions fréquemment posées

Cette section contient les questions courantes sur les éléments suivants :

- Journal des événements système
- Sécurité du réseau
- Active Directory
- Connexion directe
- Ouverture de session avec une carte à puce
- Console virtuelle
- Média virtuel
- Carte SD vFlash
- Authentification SNMP
- Périphériques de stockage
- iDRAC Service Module
- RACADM
- Divers

Sujets :

- Journal des événements système
- Sécurité du réseau
- Active Directory
- Connexion directe
- Ouverture de session avec une carte à puce
- Console virtuelle
- Média virtuel
- Carte SD vFlash
- Authentification SNMP
- Périphériques de stockage
- iDRAC Service Module
- RACADM
- Divers

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 provient d'un paramètre du navigateur. Pour remédier à ce problème :

1. Dans Internet Explorer, accédez à **Outils** > **Options Internet** > **Sécurité**et sélectionnez la zone dans laquelle vous essayez d'effectuer un téléchargement.

   Par exemple, si le périphérique iDRAC se trouve sur votre Intranet local, sélectionnez **Intranet local** et cliquez sur **Personnaliser le niveau**....

2. Dans la fenêtre **Paramètres de sécurité**, sous **Téléchargements**, vérifiez que les options suivantes sont activées :
   - 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.

Sécurité du réseau

Lors de l'accès à l'interface Web d'iDRAC, un avertissement de sécurité s'affiche pour indiquer que le certificat SSL émis par l'autorité de certification (CA) n'est pas fiable.

iDRAC contient un certificat de serveur par défaut iDRAC pour protéger le réseau lors de l'accès via l'interface Web et l'interface distante RACADM. Ce certificat n'est pas émis par une autorité CA de confiance. Pour résoudre ce problème, téléversez un certificat de serveur iDRAC émis par une CA 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 d'iDRAC, un avertissement de sécurité s'affiche pour indiquer que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte iDRAC.

iDRAC inclut un certificat de serveur iDRAC par défaut pour protéger le réseau lors de l'accès à l'interface Web et à l'interface distante RACADM. Lorsque ce certificat est utilisé, le navigateur Web affiche un avertissement de sécurité, car le certificat par défaut émis pour iDRAC ne correspond pas au nom d'hôte iDRAC (par exemple, l'adresse IP).

Pour résoudre ce problème, téléversez un certificat de serveur iDRAC émis vers l'adresse ou le nom d'hôte 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 iDRAC (si le certificat est émis vers IP) ou au nom iDRAC DNS enregistré (si le certificat est émis vers le nom enregistré iDRAC).

Pour que la CSR corresponde au nom iDRAC DNS enregistré :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **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**.

Active Directory

L'ouverture de session dans Active Directory a échoué. Comment résoudre ce problème ?

Pour identifier la cause du problème, dans la page **Configuration et gestion d'Active Directory**, cliquez sur **Tester les paramètres**. Vérifiez les résultats du test et résolvez le problème. Changez la configuration et exécutez le test jusqu'à ce que l'utilisateur de test passe l'étape d'autorisation.

En général, vérifiez les éléments suivants :

- Tout en étant connecté, veillez à utiliser le nom de domaine d'utilisateur correct et non pas le nom NetBIOS. Si vous disposez d'un compte d'utilisateur iDRAC local, ouvrez une session dans iDRAC à l'aide des données d'identification locales. Après la connexion, vérifiez que :
  - L'option **Activation Active Directory** est sélectionnée dans la page **Configuration et gestion d'Active Directory**.
  - Le paramètre DNS est correct dans la page **Configuration réseau 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 utilisateur de l'ouverture de session**. À la place, sélectionnez **Définir un domaine** et saisissez le nom du domaine sur lequel 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.

L'ouverture de session Active Directory échoue si la validation de certificat est activée. Les résultats du test contiennent le message d'erreur suivant. Pourquoi et comment résoudre le problème ?

```
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, lorsqu'iDRAC établit la connexion SSL avec le serveur de répertoire, il utilise le certificat CA téléversé pour vérifier le certificat du serveur de répertoire. Les principales causes de l'échec de la validation de certification sont les suivantes :

- La date iDRAC ne se trouve pas dans la période de validité du certificat du serveur ou du certificat CA. Vérifiez l'heure iDRAC et la période de validité de votre certificat.
- Les adresses des contrôleurs de domaine définies dans iDRAC ne correspondent pas à l'objet ou à l'autre nom d'objet du certificat du serveur de répertoire. Si vous utilisez une adresse IP, lisez la question suivante. Si vous utilisez le nom de domaine complet qualifié (FQDN), veillez à utiliser le nom de domaine complet qualifié du contrôleur de domaine et non pas 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 d'objet du certificat du contrôleur de domaine. Normalement, Active Directory utilise le nom d'hôte et non pas l'adresse IP du contrôleur de domaine dans le champ Objet ou Autre nom de l'objet du certificat du contrôleur de domaine. Pour résoudre ce problème, procédez de l'une des manières suivantes :

- Définissez le nom d'hôte (nom de domaine complet qualifié) du contrôleur de domaine comme *adresse(s) de contrôleur de domaine* dans 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 d'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 les utilisateurs et les groupes de rôles appartiennent à des domaines différents, une adresse (ou plusieurs adresses) de catalogue global est nécessaire. Dans ce cas, vous pouvez utiliser uniquement le groupe universel.

Si vous utilisez le schéma standard et que tous les utilisateurs et groupes de rôles proviennent du même domaine, une ou des adresses du catalogue global ne sont pas requises.

Si vous utilisez le schéma étendu, l'adresse du catalogue global n'est pas utilisée.

Comment fonctionne la requête de schéma standard ?

iDRAC se connecte tout d'abord à l'adresse (ou aux adresses) de contrôleur de domaine définie. Si l'utilisateur et les groupes de rôles se trouvent dans ce domaine, les privilèges sont enregistrés.

Si une adresse (ou des adresses) de contrôleur global est configurée, iDRAC continue d'interroger le catalogue global. Si des privilèges supplémentaires sont extraits du catalogue global, ces privilèges sont accumulés.

iDRAC utilise-t-il toujours LDAP sur SSL ?

Oui. Tout le transport s'effectue sur le port 636 et/ou 3 269. Au cours du test, 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 ?

iDRAC applique une sécurité stricte pour garantir l'identité du contrôleur de domaine auquel iDRAC se connecte. Sans la validation de certificat un intrus peut usurper l'identité d'un contrôleur de domaine et détourner la connexion SSL. Si vous faites confiance à tous les contrôleurs de domaine dans votre limite de sécurité sans la validation de certificat, vous pouvez la désactiver via l'interface Web ou l'interface RACADM.

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 ?

L'ouverture de session par carte à puce ou connexion directe Active Directory dure moins de 10 secondes normalement, mais elle peut prendre jusqu'à quatre minutes si vous avez défini le serveur DNS préféré et le serveur DNS secondaire et qu'une erreur s'est produite au niveau du serveur DNS préféré. Des expirations DNS se produisent lorsqu'un serveur DNS est arrêté. iDRAC vous connecte à l'aide du serveur DNS secondaire.

Active Directory est configuré pour un domaine présent dans Active Directory Windows Server 2008. Un domaine enfant ou un sous-domaine est présent pour le domaine, l'utilisateur et le groupe sont présents dans le même domaine enfant et

l'utilisateur est membre du groupe. Lors de l'ouverture d'une session dans iDRAC en utilisant l'utilisateur présent dans le domaine enfant, l'ouverture de session par connexion directe Active Directory échoue.

Ce problème peut être provoqué par un type de groupe incorrect. Il existe deux types de groupes dans le serveur Active Directory :

- Sécurité : les groupes de sécurité permettent de gérer l'accès des utilisateurs et des ordinateurs aux ressources partagées et de filtrer les paramètres de stratégies de groupe.
- Distribution : les groupes de distribution servent exclusivement de listes de distribution par e-mail.

Veillez à toujours utiliser le type de groupe Sécurité. Vous ne pouvez pas utiliser des groupes de distribution pour affecter des droits à un objet. Utilisez-les pour filtrer les paramètres de stratégie de groupe.

Connexion directe

L'ouverture de session par connexion directe échoue sur Windows Server 2008 R2 x64. Quels sont les paramètres à définir pour résoudre le problème ?

1. Exécutez **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** pour le contrôleur de domaine et la stratégie de contrôleur et de domaine.
2. Configurez les ordinateurs pour qu'ils utilisent la suite de chiffrement DES-CBC-MD5.

   Ces paramètres peuvent affecter la compatibilité avec les ordinateurs clients ou les services et les applications de votre environnement. L'option de configuration des types de chiffrement autorisés pour le paramétrage de stratégie Kerberos se trouve dans**Configuration de l'ordinateur** > **Paramètres de sécurité** > **Stratégies locales** > **Options de sécurité**.
3. Vérifiez que les clients du domaine disposent de l'objet de stratégie de groupe à jour.
4. Sur la ligne de commande, tapez `gpupdate /force` et supprimez l'ancien fichier keytab avec la commande `klist purge`.
5. Après avoir mis à jour l'objet de stratégie de groupe, créez le nouveau fichier keytab.
6. Téléversez le fichier keytab vers 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 cryptage pour Windows 7 et Windows Server 2008 R2. Pour activer les types de cryptage :

1. Ouvrez une session comme administrateur ou utilisateur doté du privilège d'administration.
2. Accédez à **Démarrer** et exécutez **gpedit.msc**. La fenêtre de **Éditeur de stratégie de groupe** s'affiche.
3. Accédez à **Paramètres de l'ordinateur local** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Options de sécurité.**.
4. Cliquez avec le bouton droit de la souris sur **Sécurité réseau : Configurer les types de cryptage autorisés pour Kerberos** et sélectionnez **Propriétés**.
5. Activez toutes les options.
6. Cliquez sur **OK**. Vous pouvez désormais ouvrir une session dans iDRAC via la connexion directe (SSO).

Définissez les paramètres supplémentaires suivants pour le schéma étendu :

1. Dans la fenêtre de **Éditeur de stratégie de groupe locale**, accédez à **Paramètres de l'ordinateur local** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Options de sécurité**.
2. Cliquez avec le bouton droit de la souris sur **Sécurité réseau : Restreindre NTLM : trafic NTLM sortant vers le serveur distant** et sélectionnez **Propriétés**.
3. Cliquez sur **Autoriser tous**, puis sur **OK** et fermez la fenêtre **Éditeur de stratégie de groupe local**.
4. Accédez à **Démarrer** et exécutez cmd. La fenêtre de l'invite de commande s'affiche.
5. Exécutez la commande `gpupdate /force`. Les stratégies de groupe sont mises à jour. Fermez la fenêtre de l'invite de commande.
6. Accédez à **Démarrer** et exécutez regedit. La fenêtre **Éditeur de registre** s'affiche.
7. Accédez à **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Control** > **LSA**.
8. Dans le volet de droite, cliquez avec le bouton droit de la souris et sélectionnez .**Nouvelle** > **Valeur DWORD (32 bits)**.
9. Nommez la nouvelle clé **SuppressExtendedProtection**.
10. Cliquez avec le bouton droit de la souris sur **SuppressExtendedProtection** et cliquez sur **Modifier.**
11. Dans le champ de données **Valeur**, tapez **1** et cliquez sur **OK**.
12. Fermez la fenêtre de l'**éditeur de registre**. Maintenant, vous pouvez ouvrir une session dans iDRAC en utilisant la connexion directe (SSO).

Si vous avez activé la connexion directe pour iDRAC et utilisez Internet Explorer pour ouvrir une session dans iDRAC, la connexion directe échoue et le système vous demande d'entrer votre nom d'utilisateur et mot de passe. Comment résoudre ce problème ?

Vérifiez que l'adresse IP d'iDRAC figure dans **Outils** > **Options Internet** > **Sécurité** > **Sites de confiance**. Si tel n'est pas le cas, la connexion directe échoue et un message vous invite à entrer votre nom d'utilisateur et votre mot de passe. Cliquez sur **Annuler** et continuez.

Ouverture de session 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.

L'ouverture de session normale par carte à puce Active Directory prend moins de 10 secondes. Cependant, elle peut prendre jusqu'à quatre minutes si vous avez défini le serveur DNS préféré et le serveur DNS secondaire dans la page **Réseau** et que le serveur DNS a échoué. Des expirations DNS se produisent lorsqu'un serveur DNS est arrêté. iDRAC vous connecte en utilisant le serveur DNS secondaire.

Le plug-in ActiveX ne parvient pas à détecter le lecteur de carte à puce

Vérifiez que la carte à puce est compatible avec le système d'exploitation Microsoft Windows. Windows prend en charge un nombre limité de fournisseurs de services cryptographiques (CSP).

En règle générale, vérifiez si les CSP de cartes à puce sont présents sur un client, insérez la carte à puce dans le lecteur lorsque l'écran d'ouverture de session de Windows apparaît (Ctrl-Alt-Suppr) et vérifiez si Windows détecte la carte à puce et affiche la boîte de dialogue du code PIN.

Le code PIN de la carte à puce est incorrect.

Déterminez si la carte à puce est verrouillée suite à un trop grand nombre de tentatives avec un code PIN incorrect. Dans ce cas, contactez l'émetteur de la carte à puce de l'entreprise pour obtenir une nouvelle carte.

Console virtuelle

Une session de console virtuelle est active, même si vous avez fermé la session dans l'interface web d'iDRAC. Est-ce normal ?

Oui Fermez la fenêtre du visualiseur de console virtuelle pour quitter la session correspondante.

Est-il possible de démarrer une nouvelle session vidéo de console distante lorsque la vidéo sur le serveur local est désactivée ?

Oui

Pourquoi la vidéo sur le serveur local prend-elle 15 secondes pour s'arrêter après la demande d'arrêt ?

Ceci permet à l'utilisateur local d'agir avant l'arrêt de la vidéo

Existe-t-il un délai lors de l'activation de la vidéo locale ?

Non, la vidéo démarre immédiatement après réception par 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 ?

Non.

L'arrêt de la console locale désactive-t-il la vidéo dans la session de console distante ?

Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de console distante.

Quels sont les privilèges nécessaires à un utilisateur 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 Telnet, 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 du moniteur de la station de gestion est 1 280 x 1 024.

Pourquoi la fenêtre du visualiseur de la console virtuelle est-elle illisible sur Linux ?

Le visualiseur de console 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 **Mouse Acceleration (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 **Single Cursor (Pointeur unique)** sous **Tools (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 système minimale requise pour que la station de gestion puisse exécuter la console virtuelle ?

La station de gestion nécessite un processeur Intel Pentium III 500 MHz avec au moins 256 Mo de RAM.

Pourquoi la fenêtre du visualiseur de console virtuelle affiche-t-elle parfois le message Aucun signal ?

Ce message peut s'afficher si le plug-in de console virtuelle 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 de rafraîchissement, 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.

Lors du démarrage d'une session de console virtuelle à partir de l'interface web d'iDRAC, un message contextuel de sécurité ActiveX apparaît. Pourquoi ?

iDRAC peut ne pas figurer dans la liste des sites de confiance. Pour que ce message n'apparaisse pas à chaque fois que vous lancez une session de console virtuelle, ajoutez iDRAC à la liste des sites de confiance dans le navigateur client :

1. Cliquez sur **Outils** > **Options Internet** > **Sécurité** > **Sites de confiance**.
2. Cliquez sur **Sites** et entrez l'adresse IP ou le nom DNS d'iDRAC.
3. Cliquez sur **Ajouter**.
4. Cliquez sur **Niveau personnalisé**.
5. Dans la fenêtre **Paramètres de sécurité**, sélectionnez **Demander** sous **Télécharger les contrôles ActiveX non signés**.

Pourquoi la fenêtre du visualiseur de console virtuelle est-elle vide ?

Si vous disposez du privilège Média Virtuel, mais pas du privilège Console virtuelle, vous pouvez démarrer le visualiseur pour accéder à la fonction Média Virtuel, mais la console du serveur géré ne s'affiche pas.

La souris ne se synchronise pas sous DOS pendant l'utilisation de la console virtuelle. Pourquoi ?

Le BIOS Dell émule le pilote de la souris comme souris PS/2. La souris PS/2 est conçue pour utiliser la position relative de son pointeur, ce qui produit un délai de synchronisation. L'iDRAC a un pilote de souris USB qui permet d'utiliser la position absolue et un meilleur suivi 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.

Lorsque la console virtuelle est lancée avec le plug-in Java dans RHEL 7.3 MS, le bouton Fermer peut ne pas être disponible pour les fenêtres de la messagerie instantanée, des performances et des statistiques.

Utilisez les touches de raccourci clavier Alt+F4 pour fermer la fenêtre.

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 **Mouse Mode (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.

Lorsque l'interface web d'iDRAC est démarrée depuis l'interface web CMC peu après le démarrage de la console virtuelle, pourquoi la session d'interface graphique expire-t-elle ?

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 fonction SysRq n'est pas prise en charge actuellement par Internet Explorer et Java.

Pourquoi le message « Liaison interrompue » s'affiche-t-il dans le bas de la console virtuelle ?

Lorsque vous utilisez le port réseau partagé au cours d'un redémarrage du serveur, iDRAC est déconnecté 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 STP (Spanning Tree Protocol) 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.

Échec du lancement de la console virtuelle avec HTML5 lorsque le navigateur est configuré de manière à utiliser uniquement TLS 1.0.

Vérifiez que le navigateur est configuré pour utiliser TLS 1.1 ou version supérieure.

Le clavier macro Win - P n'est pas disponible dans la console virtuelle une fois que le micrologiciel iDRAC est mis à jour vers 2.60.60.60.

Une version plus ancienne du contrôle Active X peut provoquer ce problème. Pour résoudre ce problème, supprimez l'extension **Contrôle ActiveX AvctViewerAPP** à partir de la page **Gérer les extensions** dans le navigateur web. Ensuite, redémarrez le navigateur et accédez à la console virtuelle. La version la plus récente du contrôle ActiveX AvctViewerAPP s'installe automatiquement.

Média virtuel

Pourquoi la connexion du client Virtual Media s'interrompt-elle parfois ?

- Si le délai d'attente du réseau expire, le micrologiciel d'iDRAC interrompt la connexion en déconnectant la liaison entre le serveur et le lecteur virtuel.
- La désactivation de la console virtuelle peut entraîner la déconnexion de la session de média virtuel. La désactivation de la vérification de révocation de certificat TLS permet d'éviter toute déconnexion. Pour désactiver le contrôle de révocation de certification TLS :
  1. Démarrez le **Panneau de configuration Java**.
  2. Cliquez sur l'onglet **Avancé**.
  3. Recherchez l'option **Vérifier la révocation du certificat TLS**, puis sélectionnez **Ne pas vérifier**.
  4. Cliquez sur **Appliquer**, puis sur **OK**. La fenêtre **Panneau de configuration Java** se ferme.
- 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 micrologiciel 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 **Client View (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 du réseau. La fenêtre d'installation n'indique pas l'avancement de l'installation.

Comment configurer le périphérique virtuel comme périphérique amorçable ?

Sur le système géré, accédez à la configuration du BIOS et au menu de démarrage. Recherchez le CD virtuel, la disquette virtuelle ou l'unité vFlash 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 de périphérique affecté au *lecteur de CD virtuel Dell*.
5. Vérifiez que le lecteur de CD virtuel est connecté.
6. Dans l'invite Linux, exécutez la commande suivante :

```
mount /dev/sdx /mnt/CD
```

   où `/dev/sdx` est le nom 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 micrologiciel à distance à l'aide de l'interface Web iDRAC ?

Les mises à jour du micrologiciel 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 et vFlash 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 ou une unité USB vFlash au bus USB hôte ou le déconnectez, toutes les unités Virtual Media et vFlash 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 ou vFlash. 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 cryptage pour Virtual Media et la console virtuelle.

REMARQUE : Dans ce cas, le transfert des 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 **Start (Démarrer)** > **Administrative Tools (Outils**

d'administration) > **Services**. Cliquez avec le bouton droit sur **Windows Event Collector (Collecteur d'événements de Windows)** et cliquez sur **Stop (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.

Échec du lancement de Virtual Media avec HTML5 lorsque le navigateur est configuré de manière à utiliser uniquement TLS 1.0.

Vérifiez que le navigateur est configuré pour utiliser TLS 1.1 ou version supérieure.

Carte SD vFlash

Quand la carte SD vFlash est-elle verrouillée ?

Elle est verrouillée lorsqu'une opération est en cours, par exemple, pendant une initialisation.

Authentification SNMP

Pourquoi le message « Accès distant : échec de l'authentification SNMP »' s'affiche-t-il ?

Lors de la découverte, l'Assistant IT tente de vérifier les noms de communauté get et set du périphérique. L'Assistant IT contient le nom de communauté get = public et le nom de communauté set = private. Par défaut, le nom de communauté d'agent SNMP pour l'agent iDRAC est public. Lorsque l'Assistant IT envoie une demande set, l'agent iDRAC génère l'erreur d'authentification SNMP, car il accepte les demandes uniquement de community = public.

Pour éviter les erreurs d'authentification SNMP, vous devez entrer les noms de communauté acceptés par l'agent. Comme iDRAC n'autorise qu'un seul nom de communauté, vous devez utiliser le même nom de communauté get et set pour la configuration de découverte de l'Assistant IT.

Périphériques de stockage

Les informations sur tous les périphériques de stockage connectés au système ne sont pas affichées et OpenManage Storage Management affiche plus de périphériques de stockage qu'iDRAC. Pourquoi ?

iDRAC affiche des informations uniquement pour les périphériques pris en charge CEM (Comprehensive Embedded Management).

iDRAC Service Module

Avant d'installer ou d'exécuter l'iDRAC Service Module, l'Open Manage Server Administrator doit-il être désinstallé ?

Non, vous n'avez pas besoin de désinstaller Server Administrator. Avant d'installer ou d'exécuter l'iDRAC Service Module, assurez-vous que vous avez arrêté les fonctions de Server Administrator que fournit l'iDRAC Service Module.

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**, 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 affiché est **installé**.

REMARQUE : Pour vérifier si 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 de l'iDRAC Service Module installée apparaît dans l'onglet **Version**.
- Accédez à **Poste de travail** > **Désinstaller ou modifier un programme**.

Quel est le niveau d'autorisation minimal requis pour installer l'iDRAC Service Module ?

Pour installer l'iDRAC Service Module, vous devez disposer de privilèges Administrateur.

Sur iDRAC Service Module version 2.0 et versions antérieures, lors de l'installation d'iDRAC Service Module, un message d'erreur s'affiche indiquant ce n'est pas un serveur pris en charge. Consultez le Guide d'utilisation pour en savoir plus sur les serveurs pris en charge. Comment résoudre cette erreur ?

Avant d'installer iDRAC Service Module, assurez-vous que le serveur est un serveur PowerEdge de 12e génération ou de version ultérieure. En outre, assurez-vous que vous disposez d'un système 64 bits.

Le message suivant s'affiche dans le journal du système d'exploitation, même si la fonction de connexion directe entre l'OS 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 le tableau d'acheminement 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 d'acheminement.

Tableau 48. Module des services des iDRAC (iSM)

Destination	Passerelle	Masque générique	Indicateurs	Mesure	Réf.	Utiliser Iface
Par défaut	10.94.148.1	0.0.0.0	UG	1 024	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 SE et iDRAC. Pour résoudre le problème de connexion, assurez-vous que l'adresse IPv4 USBNIC iDRAC (la valeur par défaut est 169.254.0.1) 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 d'acheminement 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.

Lors de la désinstallation de l'iDRAC Service Module version 2.0 et versions antérieures à partir d'un serveur VMware ESXi, le commutateur virtuel est nommé comme vSwitchiDRACvusb et groupe de ports en tant que Réseau iDRAC dans le client vSphere. Comment faire pour les supprimer ?

Lors de l'installation du VIB de l'iDRAC Service Module sur un serveur ESXi VMware, l'iDRAC Service Module crée le vSwitch et Portgroup pour communiquer avec iDRAC via la fonction Connexion directe entre le SE et iDRAC en mode NIC USB. Après la désinstallation, le commutateur virtuel **vSwitchiDRACvusb** et le groupe de ports **réseau iDRAC** ne sont pas supprimés. Pour les supprimer manuellement, effectuez l'une des opérations suivantes :

- Accédez à l'Assistant Configuration du client vSphere et supprimez les entrées.
- Accédez au Esxcli et tapez les commandes suivantes :
  - Pour supprimer un groupe de ports : `esxcfg-vmknic -d -p "iDRAC Network"`
  - Pour retirer le commutateur virtuel vSwitch : `esxcfg-vswitch -d vSwitchiDRACvusb`

REMARQUE : Vous pouvez réinstaller l'iDRAC Service Module sur le serveur ESXi VMware car il ne s'agit pas d'un problème fonctionnel du serveur.

Où se trouve le journal Lifecycle répliqué sur le système d'exploitation ?

Pour afficher les journaux Lifecycle Controller répliqués :

Tableau 49. les journaux Lifecycle ;

Système d'exploitation	Emplacement
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**. **REMARQUE :** Dans iSM version 2.1 et versions ultérieures, les journaux Lifecycle sont répliqués sous le nom de la source du journal Lifecycle Controller. Dans iSM version 2.0 et versions antérieures, les journaux sont répliqués sous le nom de la source d'iDRAC Service Module. **REMARQUE :** L'emplacement du journal Lifecycle peut être configuré à l'aide du programme d'installation d'iDRAC Service Module. Vous pouvez configurer l'emplacement lors de l'installation de l'iDRAC Service Module ou la modification du 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 *Dépendances Linux* dans l'*iDRAC Service Module User's Guide* (Guide d'utilisation du module Service iDRAC).

RACADM

Après avoir réinitialisé 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 indique ?

```
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.

Vérifiez que les versions officielles de openssl et libopenssl sont installées. Exécutez la commande suivante pour installer les modules RPM :

```
rpm -ivh --force < filename >
```

où `filename` correspond au fichier du progiciel 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, notamment lorsque la commande `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 ?

Le message s'affiche, car l'opération de création de partition est en cours. Cependant, la partition est supprimée après un moment et un message indiquant que la partition est supprimée s'affiche. Si tel n'est pas le cas, attendez la fin de la création de la partition et supprimez la partition.

Divers

Comment rechercher l'adresse IP d'iDRAC d'un serveur lame ?

- **À l'aide de l'interface web de CMC** :

  Accédez à **Châssis** > **Serveurs** > **Configuration** > **Déployer**. Dans le tableau qui s'affiche, identifiez l'adresse IP du serveur.

- **À l'aide de Virtual Console** : redémarrez le serveur pour afficher l'adresse IP de l'iDRAC durant le test POST. Sélectionnez la console « Dell CMC » dans OSCAR pour vous connecter à CMC via une connexion série locale. Les commandes CMC RACADM peuvent être envoyées via cette connexion.

  Pour en savoir plus sur les commandes RACADM CMC, voir le *Guide de référence de l'interface de ligne de commande RACADM CMC*, disponible sur **dell.com/esmmanuals**.

  Pour en savoir plus sur les commandes RACADM iDRAC, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

- **À l'aide de RACADM local**

  Utilisez la commande `racadm getsysinfo`, par exemple :

  ```
  $ racadm getniccfg -m server-1
  DHCP Enabled = 1
  IP Address   = 192.168.0.1
  Subnet Mask  = 255.255.255.0
  Gateway      = 192.168.0.1
  ```

- **À l'aide de LCD** :

  Dans le menu principal, sélectionnez le serveur, appuyez sur le bouton de vérification, sélectionnez le serveur approprié, et appuyez sur le bouton de vérification.

Comment rechercher l'adresse IP CMC du serveur lame ?

- **Depuis l'interface web d'iDRAC** :

  Accédez à **Présentation** > **Paramètres iDRAC** > **CMC**. La page **CMC Summary (Récapitulatif CMC)** affiche l'adresse IP de CMC.

- **Depuis la console virtuelle** :

  Sélectionnez la console « Dell CMC » dans OSCAR pour vous connecter à CMC via une connexion série locale. Les commandes CMC RACADM peuvent être transmises via cette connexion.

```
$ racadm getniccfg -m chassis
NIC Enabled         = 1
DHCP Enabled        = 1
Static IP Address   = 192.168.0.120
Static Subnet Mask  = 255.255.255.0
Static Gateway      = 192.168.0.1
Current IP Address  = 10.35.155.151
Current Subnet Mask = 255.255.255.0
Current Gateway     = 10.35.155.1
Speed               = Autonegotiate
Duplex              = Autonegotiate
```

  REMARQUE : Vous pouvez également utiliser ces informations via l'interface distante RACADM.

  Pour en savoir plus sur les commandes RACADM CMC, voir le *Guide de référence de l'interface de ligne de commande RACADM CMC*, disponible sur **dell.com/esmmanuals**.

  Pour en savoir plus sur les commandes RACADM iDRAC, voir le *Guide de référence de l'interface de ligne de commande RACADM iDRAC*, disponible sur **dell.com/idracmanuals**.

Comment rechercher l'adresse IP iDRAC IP d'un serveur en rack ou de type tour ?

- **Depuis l'interface web d'iDRAC** :

  Accédez à **Présentation** > **Serveur** > **Propriétés** > **Récapitulatif**. La page **Récapitulatif du système** affiche l'adresse IP d'iDRAC.

- **À partir de RACADM local** :

  Utilisez la commande `racadm getsysinfo`.

- **Depuis LCD** :

  Sur le serveur physique, utilisez les boutons de navigation du panneau LCD pour afficher l'adresse IP de l'iDRAC. Accédez à **Setup View (Vue configuration)** > **View (Afficher)** > **iDRAC IP (IP iDRAC)** > **IPv4** ou **IPv6** > **IP**.

- **Depuis OpenManage Server Administrator** :

  Dans l'interface Web de Server Administrator, accédez à **Boîtier modulaire** > **Système/Module serveur** > **Châssis du système principal/Système principal** > **Accès distant**.

La connexion réseau iDRAC ne fonctionne pas.

Pour les serveurs lames :

- Assurez-vous que le câble LAN est connecté à CMC.
- Assurez-vous que les paramètres NIC, les paramètres IPv4 ou IPv6 et que Statique ou DHCP est activé pour votre réseau.

Pour les serveurs en rack et de type tour :

- En mode partagé, vérifiez que le câble LAN est 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.

Le serveur lame est inséré dans le châssis, mais l'actionnement du bouton Marche/Arrêt ne met pas le serveur sous tension

- iDRAC nécessite deux minutes pour s'initialiser avant la mise sous tension du serveur.
- Vérifiez la consommation énergétique du CMC. La consommation énergétique du châssis a peut-être dépassé la limite.

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.

Comment changer le nom du logement du système dans un châssis ?

1. Ouvrez une session dans l'interface web CMC et accédez à **Châssis** > **Serveurs** > **Installation**.
2. Entrez le nouveau nom du logement dans la ligne du serveur et cliquez sur **Appliquer**.

iDRAC sur le serveur lame ne répond pas au cours du démarrage.

Retirez et réinsérez le serveur.

Consultez l'interface Web CMC pour déterminer si l'iDRAC s'affiche comme composant pouvant être mis à niveau. Si tel est le cas, suivez les instructions de la section Mise à jour du micrologiciel à l'aide de l'interface Web CMC.

Si le problème persiste, contactez le support technique.

Lors de la tentative de démarrage du serveur géré, le voyant d'alimentation est vert, mais aucun POST ou aucune vidéo ne s'affiche.

Ce problème apparaît pour l'une des raisons suivantes :

- La mémoire n'est pas installée ou elle est inaccessible.
- Le processeur n'est pas installé ou il est inaccessible.
- La carte complémentaire vidéo n'est pas installée ou elle n'est pas connectée correctement.

Consultez également les messages d'erreur dans le journal iDRAC en utilisant l'interface web d'iDRAC ou l'écran LCD du serveur.

25

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
- Obtention des informations système et évaluation de l'intégrité du système
- Définition des alertes et configuration des alertes par e-mail
- Affichage et exportation du journal Lifecycle et du journal des événements système
- Interfaces de mise à niveau du micrologiciel iDRAC
- Exécution d'un arrêt normal
- Création d'un compte utilisateur Administrateur
- Lancement de la console distante du serveur et montage d'un lecteur USB
- Installation d'un système d'exploitation nu à l'aide d'un média virtuel connecté et du partage de fichier à distance
- Gestion de la densité d'un rack
- Installation d'une nouvelle licence électronique
- Application des paramètres de configuration d'identité d'E/S pour plusieurs cartes réseau lors du redémarrage d'un système hôte unique

Dépannage d'un système géré inaccessible

Après avoir reçu des alertes d'OpenManage Essentials, de Dell Management Console ou d'un collecteur d'interruptions local, cinq serveurs dans un centre de données sont inaccessibles suite à un blocage du système d'exploitation ou du serveur. Il est nécessaire d'identifier l'origine du problème et de démarrer le serveur à l'aide d'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 :

REMARQUE : Si vous ne pouvez pas vous connecter à l'interface Web iDRAC, accédez au panneau LCD, notez l'adresse IP ou le nom d'hôte, puis exécutez les opérations suivantes à l'aide de l'interface Web iDRAC depuis la station de gestion :

- État du voyant du serveur : orange clignotant ou orange fixe.
- État de l'écran LCD du panneau avant : LCD orange ou message d'erreur.
- L'image du système d'exploitation figure dans la console virtuelle. Si vous pouvez voir l'image (démarrage à chaud), ouvrez une nouvelle session. Si vous pouvez ouvrir une session, le problème est résolu.
- Écran du dernier blocage
- Vidéo de capture de démarrage.
- Vidéo de capture de blocage.
- État d'intégrité du serveur : icônes *x* rouges pour les composant défaillants.
- État de la baie de stockage : baie éventuellement hors ligne ou défaillante
- Journal Lifecycle des événements critiques liés au matériel et au micrologiciel du système et entrées de journal consignées lors du blocage du système.
- Générer un rapport de support technique et afficher les données collectées.
- Utiliser les fonctions de surveillance offertes par l'iDRAC Service Module

Tâches associées

Prévisualisation de la console virtuelle , page 239

Affichage des vidéos de capture de démarrage et de blocage , page 299

Affichage de l'intégrité du système , page 301

Affichage des journaux , page 299

Génération de la collecte SupportAssist , page 302
Inventaire et surveillance des périphériques de stockage , page 207
Utilisation de l'iDRAC Service Module , page 275

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 iDRAC, accédez à **Présentation** > **Serveur** > **Récapitulatif du système** pour afficher les informations du système et accéder aux liens de la page pour évaluer l'intégrité du système. Par exemple, vous pouvez évaluer l'intégrité du ventilateur du châssis.
- Vous pouvez également configurer le voyant d'emplacement dans le châssis et, en fonction de la couleur, évaluer l'intégrité du système.
- Si l'iDRAC Service Module est installé, les informations d'hôte du système d'exploitation s'affichent.

Tâches associées

Affichage de l'intégrité du système , page 301
Utilisation de l'iDRAC Service Module , page 275
Génération de la collecte SupportAssist , page 302

Définition des alertes et configuration des alertes par e-mail

Pour définir des alertes et des alertes par e-mail :

1. Activez les alertes.
2. Configurez l'alerte par e-mail et vérifiez les ports.
3. Redémarrez le système géré, mettez-le hors tension ou exécutez un cycle d'alimentation sur le système géré.
4. Envoyez une alerte de test.

Affichage et exportation du journal Lifecycle et du journal des événements système

Pour afficher et exporter le journal Lifecycle et le journal des événements système (SEL) :

1. Dans l'interface Web iDRAC, accédez à **Présentation** > **Serveur** > **Journaux**pour afficher le journal SEL, et **Présentation** > **Serveur** > **Journaux** > **Journal Lifecycle** pour afficher le journal Lifecycle.

   REMARQUE : Le journal est également enregistré dans le journal Lifecycle. Utilisez les options de filtrage pour afficher le journal SEL.

2. Exportez le journal SEL ou Lifecycle au format XML vers un emplacement externe (station de gestion, USB, partage de réseau, etc.). Vous pouvez également activer la journalisation sur un système distant pour que tous les journaux écrits dans le journal Lifecycle soient écrits également simultanément sur le ou les serveurs distants configurés.
3. Si vous utilisez l'iDRAC Service Module, exportez le journal Lifecycle vers le journal du système d'exploitation. Pour plus d'informations, voir Utilisation de l'iDRAC Service Module , page 275.

Interfaces de mise à niveau du micrologiciel iDRAC

Utilisez les interfaces suivantes pour mettre à jour le micrologiciel iDRAC :

- l'interface Web iDRAC
- CLI RACADM (iDRAC et CMC)

- Progiciel de mise à jour Dell (DUP - Dell Update Package)
- Interface Web CMC
- Services à distance Lifecycle Controller
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Exécution d'un arrêt normal

Pour exécuter un arrêt normal, dans l'interface web d'iDRAC, accédez aux emplacements suivants :

- **Présentation générale** > **Serveur** > **Alimentation/Thermique** > **Configuration de l'alimentation** > **Contrôle de l'alimentation**. La page **Contrôle de l'alimentation** s'affiche. Sélectionnez **Arrêt normal** et cliquez sur **Appliquer**.
- **Présentation** > **Serveur** > **Alimentation/Thermique** > **Surveillance de l'alimentation**. Dans le menu déroulant **Contrôle de l'alimentation**, sélectionnez **Arrêt normal**, puis cliquez sur **Appliquer**.

REMARQUE : Toutes les options d'**alimentation** dépendent du système d'exploitation hôte. Pour qu'elles fonctionnent correctement, vous devez procéder dans le système d'exploitation aux modifications requises. Par exemple, dans RHEL 7.2, l'outil Gnome-tweak-tool.

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

Création d'un compte utilisateur Administrateur

Vous pouvez modifier le compte utilisateur Administrateur par défaut ou créer un compte d'administrateur. Pour modifier le compte d'administrateur local, voir Modification des paramètres du comptes d'administrateur.

Pour créer un compte d'administrateur, voir les sections suivantes :

- Configuration des utilisateurs locaux
- Configuration des utilisateurs d'Active Directory
- Configuration d'utilisateurs LDAP générique

Lancement de la console distante du serveur et montage d'un lecteur USB

Pour lancer la console distante et monter un lecteur USB :

1. Connectez un lecteur Flash USB (avec l'image nécessaire) à la station de gestion.
2. Utilisez les méthodes suivantes pour lancer la console virtuelle via l'interface Web iDRAC :
   - Allez à **Présentation générale** > **Serveur** > **Console virtuelle** et cliquez sur **Lancer la console virtuelle**.
   - Accédez à **Présentation générale** > **Serveur** > **Propriétés** et cliquez sur **Lancer** sous **Prévisualisation de la console virtuelle**.

   Le **Visualiseur de console virtuelle** s'affiche.
3. Dans le menu **Fichier**, cliquez sur **Média Virtuel** > **Lancer Média Virtuel**.
4. Cliquez sur **Ajouter une image** et sélectionnez l'image qui se trouve sur le lecteur Flash USB.
   L'image est ajoutée à la liste des lecteurs disponibles.
5. Sélectionnez le lecteur à lui associer. L'image sur le lecteur Flash USB est associée au système géré.

Installation d'un système d'exploitation nu à l'aide d'un média virtuel connecté et du partage de fichier à distance

Voir Déploiement d'un système d'exploitation à l'aide du partage de fichier à distance.

Gestion de la densité d'un rack

Actuellement, les deux serveurs sont installés dans un rack. Pour ajouter deux serveurs, vous devez déterminer la capacité restante dans le rack.

Pour évaluer la capacité d'un rack pour ajouter des serveurs :

1. Affichez les données de consommation électrique actuelle et l'historique de consommation des serveurs.
2. En fonction des données, de l'infrastructure d'alimentation et des limitations du système, activez la stratégie de limitation de puissance et définissez les valeurs correspondantes.

   REMARQUE : Il est recommandé de définir une limite proche du pic, puis d'utiliser le niveau limité pour déterminer la capacité restante dans le rack pour ajouter des serveurs.

Installation d'une nouvelle licence électronique

Voir Opérations de licence pour plus d'informations.

Application des paramètres de configuration d'identité d'E/S pour plusieurs cartes réseau lors du redémarrage d'un système hôte unique

Si vous disposez de plusieurs cartes réseau dans un serveur qui fait partie d'un environnement SAN (Storage Area Network) et que vous souhaitez leur appliquer différents paramètres d'adresse virtuelle, d'initiateur et de configuration cible, utilisez la fonction d'optimisation d'identité d'E/S pour réduire le temps de configuration des paramètres. Pour ce faire :

1. Assurez-vous que le BIOS, l'iDRAC et les cartes réseau sont mis à jour à la dernière version du micrologiciel.
2. Activez l'optimisation d'identité ES.
3. Exportez le fichier de configuration XML à partir d'iDRAC.
4. Modifiez les paramètres d'optimisation d'identité d'E/S dans le fichier XML.
5. Importez le fichier de configuration XML sur l'iDRAC.

Concepts associés

Mise à jour du micrologiciel de périphérique , page 64
Activation ou désactivation de l'optimisation d'identité d'E/S , page 189