Dell OpenManage Server Administrator Version 7.3
Guide d'utilisation

Remarques, précautions et avertissements

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

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

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

2013 - 06

Rév. A00

Table des matières

1

Introduction

Dell OpenManage Server Administrator (OMSA) fournit une solution de gestion des systèmes un à un exhaustive de deux façons : depuis une interface utilisateur graphique (GUI) intégrée basée sur le navigateur Web et depuis une interface de ligne de commande (CLI) via le système d'exploitation. Server Administrator permet aux administrateurs du système de gérer les systèmes localement ou à distance sur un réseau. Cela permet aux administrateurs du système de se concentrer sur la gestion de l'intégralité du réseau en fournissant une gestion des systèmes un à un exhaustive. Dans le contexte de Server Administrator, un système fait référence à un système autonome, un système dont les unités de stockage reliées sur le réseau se trouvent sur un châssis distinct, ou un système modulaire comprenant un ou plusieurs modules de serveur dans une enceinte modulaires. Server Administrator fournit des informations sur :

- Les systèmes qui fonctionnent correctement et ceux qui sont défectueux ;
- Les systèmes nécessitant des opérations de restauration à distance

Server Administrator offre une gestion et une administration faciles des systèmes locaux et à distance via un ensemble de services de gestion intégrés exhaustifs. Server Administrator est la seule installation du système gérée et accessible localement et à distance depuis la page d'accueil **Server Administrator**. Les systèmes surveillés à distance sont accessibles via des connexions de numérotation, LAN ou sans fil. Server Administrator assure la sécurité de ses connexions de gestion via le contrôle d'accès basé sur les rôles (RBAC), l'authentification et le cryptage SSL (secure socket layer).

Installation

Vous pouvez installer Server Administrator à l'aide du DVD *Dell Systems Management Tools and Documentation* (Outils et documentation de gestion des systèmes Dell). Le DVD fournit un programme de configuration pour installer, mettre à niveau ou désinstaller les composants logiciels de Server Administrator, du système géré et de la station de gestion. En outre, vous pouvez installer Server Administrator sur plusieurs systèmes via une installation automatique sur un réseau. Le programme d'installation de Dell OpenManage fournit des scripts d'installation et des progiciels RPM pour installer et désinstaller Dell OpenManage Server Administrator et d'autres composants logiciels de système géré sur votre système géré. Pour en savoir plus, voir le *Dell OpenManage Server Administrator Installation Guide* (Guide d'installation de Dell OpenManage Server Administrator) et le *Dell OpenManage Management Station Software Installation Guide* (Guide d'installation du logiciel de la station de gestion Dell OpenManage) à l'adresse **dell.com/support/manuals**.

REMARQUE : Lorsque vous installez les progiciels « open source » depuis le DVD *Dell Systems Management Tools and Documentation* (Outils et documentation de gestions des systèmes Dell), les fichiers de licence correspondants sont automatiquement copiés sur le système. Lorsque vous supprimez ces progiciels, les fichiers correspondants sont également supprimés.

REMARQUE : Si vous disposez d'un système modulaire, vous devez installer Server Administrator sur chaque module de serveur installé dans le châssis.

Mise à jour de composants système particuliers

Pour mettre à jour les composants système particuliers, utilisez les DUP (progiciels de mise à jour Dell) spécifiques aux composants. Utilisez le DVD *Dell Server Update Utility* pour afficher le rapport de version complet et pour mettre à jour

un système dans son intégralité. L'utilitaire SUU (Server Update Utility) identifie et applique les mises à jour requises sur votre système. L'utilitaire SUU est également téléchargeable depuis **support.dell.com.**

REMARQUE : Pour en savoir plus sur l'obtention et l'utilisation de l'utilitaire SUU, sur la mise à jour des systèmes Dell ou sur la consultation des mises à jour disponibles pour tout système répertorié dans l'espace de stockage, consultez le *Dell Server Update Utility User's Guide* (Guide d'utilisation de l'utilitaire SUU) à l'adresse **dell.com/support/manuals**.

Storage Management Service (Service de gestion de stockage)

Le service de gestion du stockage (Storage Management Service) fournit des informations de gestion du stockage sur un affichage graphique intégré.

REMARQUE : Pour des informations détaillées sur Storage Management Service, voir le *Dell OpenManage Server Administrator Storage Management User's Guide*(Guide d'utilisation de Dell OpenManage Server Administrator Storage Management) sur à l'adresse **dell.com/support/manuals**.

Instrumentation Service

Instrumentation Service fournit un accès rapide à des informations détaillées sur les défaillances et les performances recueillies par des agents de gestion de systèmes standard de l'industrie et permet l'administration à distance de systèmes surveillés, y compris l'arrêt, le démarrage et la sécurité.

Contrôleur d'accès à distance (RAC)

Le contrôleur d'accès à distance fournit une solution de gestion de système à distance complète pour les systèmes équipés du contrôleur DRAC (Dell Remote Access Controller) ou BMC (Baseboard Management Controller)/iDRAC (Integrated Dell Remote Access Controller). Le contrôleur d'accès à distance permet d'accéder à distance à un système inopérant, vous permettant ainsi de corriger et redémarrer le système dans les plus brefs délais. Le contrôleur d'accès à distance fournit également une notification d'alerte lorsqu'un système est en arrêt et vous permet de le redémarrer à distance. En outre, le contrôleur d'accès à distance journalise la cause possible de l'arrêt du système et enregistre l'écran de panne/d'arrêt le plus récent.

Journaux

Server Administrator affiche des journaux de commandes envoyées au système ou par le système, des événements de matériel surveillés et des alertes système. Vous pouvez ouvrir ces journaux depuis la page d'accueil, ainsi que les imprimer ou enregistrer en tant que rapports, et les envoyer par e-mail à un contact de service désigné.

Nouveautés de cette version

- Prise en charge complémentaire des systèmes d'exploitation suivants :
  - Red Hat Enterprise Linux 5.9 (32 bits et 64 bits)
  - Red Hat Enterprise Linux 6.4 (64 bits)
  - Microsoft Windows Server 2012 Essentials
  - VMware vSphere 5.1 U1
  - VMware vSphere 5.0 U2
  - Citrix XenServer 6.2

- Correctifs et optimisation de sécurité pour les éléments suivants :
  - CVE-2012-6272, CSRF, XSS et manipulation de chemin d'accès généré corrigés
  - Mise à niveau à JRE version 1.7 Mise à jour 21
  - Mise à niveau à Apache Tomcat version 7.0.39
- Ajout de prise en charge de Google Chrome 21 et 22
- Ajout de prise en charge de Safari 5.1.7 sur Apple Mac OS X
- Ajout de prise en charge des cartes d'interface réseau (NIC) suivantes :
  - Broadcom 57840S quatre ports 10G SFP+ Rack NDC
  - Broadcom 57840S-k quatre ports 10GbE Lame KR NDC
- Prise en charge des blocs d'alimentation CC 240 volts
- Capacité à définir les destinations d'événements de plateforme tels que IPv4, IPv6 ou FQDN sur les systèmes 12G avec des versions spécifiques d'iDRAC7
- Ajout de support des fonctions suivantes dans Storage Management:
  - Prise en charge de PCIe SSD sur ESXi 5.1 U1.
  - Condition d'endurance d'écriture nominale restante des SSD SAS et SATA liés à un PERC 8.
  - Prise en charge de Fluid Cache pour DAS (Direct Attached Storage - Stockage relié direct) sur Red Hat Enterprise Linux 6.4 et Novell SUSE Linux Enterprise Server 11 SP2 pour PERC H810, H710 Adapter, H710P et H710 Mini sur Dell PowerEdge R720, R820, R620 et T620.

    REMARQUE : Pour des informations supplémentaires, consultez le *Dell OpenManage Server Administrator Storage Management User's Guide* (Guide d'utilisation de Dell OpenManage Server Administrator Storage Management) à l'adresse **dell.com/openmanagemanuals**.
- Prise en charge dépréciée des systèmes d'exploitation suivants :
  - Red Hat Enterprise Linux 6.3
  - Red Hat Enterprise Linux 5.8

REMARQUE : Pour connaître la liste des systèmes d'exploitation et des serveurs Dell pris en charge, voir *Dell Systems Software Support Matrix* (Matrice de prise en charge logicielle des systèmes Dell) dans la version requise du logiciel OpenManage à l'adresse **dell.com/openmanagemanuals**.

REMARQUE : Pour en savoir plus sur les nouvelles fonctionnalités de cette version, voir l'aide en ligne contextuelle de Server Administrator.

Disponibilité des normes de Systems Management

Dell OpenManage Server Administrator prend en charge les protocoles de Systems Management suivants :

- Protocole HTTPS (HyperText Transfer Protocol Secure)
- Modèle commun d'informations (CIM)
- Protocole SNMP (Simple Network Management Protocol - protocole de gestion de réseau simple)

Si votre système prend en charge SNMP, vous devez installer et activer le service sur votre système d'exploitation. Si les services SNMP sont disponibles sur votre système d'exploitation, le programme d'installation de Server Administrator installe les agents pris en charge pour SNMP.

HTTPS est pris en charge sur tous les systèmes d'exploitation. La prise en charge de CIM et SNMP dépend du système d'exploitation et, dans certains cas, de la version du système d'exploitation.

REMARQUE : Pour en savoir plus sur les problèmes de sécurité SNMP, voir le fichier Lisez-moi de Dell OpenManage Server Administrator (inclus avec l'application Server Administrator) ou rendez-vous sur **dell.com/support/manuals**. Vous devez appliquer les mises à jour depuis les agents SNMP maître de votre système d'exploitation pour assurer que les sous-agents SNMP de Dell sont sécurisés.

Disponibilité sur les systèmes d'exploitation pris en charge

Sur les systèmes d'exploitation Microsoft Windows pris en charge, Server Administrator prend en charge deux normes Systems Management : CIM/WMI (Windows Management Instrumentation) et SNMP, tandis que sur les systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge, Server Administrator prend en charge la norme Systems Management SNMP.

Server Administrator ajoute une sécurité considérable à ces normes de Systems Management. Tous les opérations de définition d'attributs (par exemple, modifier la valeur d'un numéro d'inventaire) doivent être réalisées à l'aide de Dell OpenManage IT Assistant, tout en étant connecté avec les privilèges d'administrateur requis.

Le tableau suivant indique les normes de Systems Management disponibles pour chacun des systèmes d'exploitation pris en charge.

Tableau 1. Disponibilité des normes de Systems Management

Système d'exploitation	SNMP	CIM
Famille Windows Server 2008 et famille Windows Server 2003	Disponible sur le média d'installation du système d'exploitation	Toujours installé
Red Hat Enterprise Linux	Disponible dans le progiciel net-snmp du média d'installation du système d'exploitation	Non disponible
SUSE Linux Enterprise Server	Disponible dans le progiciel net-snmp du média d'installation du système d'exploitation	Non disponible
VMWare ESX	Disponible dans le progiciel net-snmp installé par le système d'exploitation	Disponible
VMWare ESXi	Prise en charge des interruptions SNMP disponible **REMARQUE :** Bien que ESXi prenne en charge les interruptions SNMP, il ne prend pas en charge l'inventaire matériel via SNMP.	Disponible
Citrix XenServer 6.0	Disponible dans le progiciel net-snmp du média d'installation du système d'exploitation	Non disponible

Page d'accueil de Server Administrator

La page d'accueil de **Server Administrator** fournit des tâches de gestion du système Web facile à configurer et à utiliser depuis le système géré ou depuis un hôte distant via un réseau LAN, un service de connexion par numérotation ou un réseau sans fil. Lorsque le Dell Systems Management Server Administrator Connection Service (service de connexion DSM SA) est installé et configuré sur le système géré, vous pouvez effectuez des actions de gestions distantes depuis tout système doté d'un navigateur Web et d'une connexion pris en charge. En outre, la page d'accueil Server Administrator fournit une aide en ligne sensible au contexte exhaustive.

Autres documents utiles

Outre ce guide, les manuels suivants sont disponibles sur **dell.com/support/manuals**.

- Le document *Dell Systems Software Support Matrix* (Matrice de prise en charge logicielle des systèmes Dell) fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- Le *Guide d'installation de Dell OpenManage Server Administrator* contient les instructions d'installation de Dell OpenManage Server Administrator.
- Le *Dell OpenManage Management Station Software Installation Guide* (Guide d'installation du logiciel de la station de gestion Dell OpenManage) contient des instructions qui vous aideront à installer le logiciel de la station de gestion Dell OpenManage.
- Le *Dell OpenManage Server Administrator SNMP Reference Guide* (Guide de référence de SNMP de Dell OpenManage Server Administrator) fournit des informations sur la base d'informations de gestion (MIB) du protocole simplifié de gestion de réseau (SNMP).
- Le *Dell OpenManage Server Administrator CIM Reference Guide* (Guide de référence CIM de Dell OpenManage Server Administrator) répertorie le fournisseur du modèle commun d'informations (CIM) et un suffixe de fichier de format d'objet de gestion standard (MOF).
- Le *Dell OpenManage Server Administrator Messages Reference Guide* (Guide de référence des messages de Dell OpenManage Server Administrator) répertorie les messages qui s'affichent dans votre journal des alertes de la page d'accueil de Server Administrator ou sur le visualiseur d'événements de votre système d'exploitation.
- Le *Dell OpenManage Server Administrator Command Line Interface Guide* (Guide d'utilisation de l'interface de ligne de commande Dell OpenManage) décrit la totalité de l'interface de ligne de commande.
- Le *Dell Remote Access Controller 5 User's Guide* (Guide d'utilisation de Dell Remote Access Controller 5) contient des informations exhaustives sur l'utilisation de l'utilitaire de ligne de commande RACADM pour configurer un DRAC 5.
- Le *Dell Chassis Management Controller User's Guide* (Guide d'utilisation de Dell Chassis Management Controller) fournit des informations exhaustives sur l'utilisation du contrôleur qui gère tous les modules du châssis contenant votre système Dell.
- Le *Command Line Reference Guide for iDRAC6 and CMC* (Guide de référence de la ligne de commande pour iDRAC6 et CMC) fournit des informations sur les sous-commandes RACADM, les interfaces prises en charge, les groupes des bases de données de propriétés et les définitions d'objets pour iDRAC6 et CMC.
- Le *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* (Guide d'utilisation Integrated Dell Remote Access Controller 7 (iDRAC7)) fournit des informations sur la configuration et l'utilisation d'iDRAC7 pour les serveurs tours, lames et racks 12G pour gérer et surveiller votre système et ses ressources partagées à distance via un réseau.
- Le *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* (Guide d'utilisation Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers) fournit des informations sur la configuration et l'utilisation d'iDRAC6 pour les serveurs lames 11G pour gérer et surveiller votre système et ses ressources partagées à distance via un réseau..
- Le *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers* (Guide d'utilisation Integrated Dell Remote Access Controller 6 (iDRAC6)) fournit des informations exhaustives sur la configuration et l'utilisation d'iDRAC6 pour les serveurs tours et racks 11G pour gérer et surveiller votre système et ses ressources partagées à distance via un réseau.
- Le *Dell Online Diagnostics User's Guide* (Guide d'utilisation de Dell Online Diagnostics) fournit des informations complètes sur l'installation et l'utilisation de Online Diagnostics sur votre système.
- Le *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Guide d'utilisation des utilitaires de Dell OpenManage Baseboard Management Controller) fournit des informations supplémentaires sur l'utilisation de Server Administrator pour configurer et gérer le contrôleur BMC de votre système.
- Le *Dell OpenManage Server Administrator Storage Management User's Guide* (Guide d'utilisation de Dell OpenManage Server Administrator Storage Management) est un guide de référence complet pour la configuration et la gestion du stockage local et distant connecté à un système.

- Le *Dell Remote Access Controller Racadm User's Guide* (Guide d'utilisation de l'utilitaire Racadm de Dell Remote Access Controller) fournit des informations sur l'utilisation de l'utilitaire de ligne de commande racadm.
- Le *Guide d'utilisation de Dell Remote Access Controller 5* fournit des informations complètes sur l'installation et la configuration d'un contrôleur DRAC 5, et sur son utilisation pour accéder à distance à un système ne fonctionnant pas.
- Le *Dell Update Packages User's Guide* (Guide d'utilisation des progiciels de mise à jour Dell) fournit des informations sur l'obtention et l'utilisation des progiciels DUP dans le cadre de la stratégie de mise à jour de votre système.
- Consultez le *Dell OpenManage Server Update Utility User's Guide* (Guide d'utilisation de l'utilitaire Dell OpenManage Server Update Utility) pour plus d'informations sur la manière d'obtenir et d'utiliser Server Update Utility (SUU) pour mettre à jour vos systèmes Dell ou pour afficher les mises à jour disponibles pour n'importe quel système répertorié dans l'espace de stockage.
- Le *Dell Management Console User's Guide* (Guide d'utilisation de Dell Management Console) fournit des informations sur l'installation, la configuration et l'utilisation de Dell Management Console.
- Le *Dell Lifecycle Controller User's Guide* (Guide d'utilisation de Dell Life Cycle Controller) fournit des informations sur la configuration et l'utilisation d'Unified Server Configurator pour effectuer des tâches de gestion de systèmes et de stockage tout au long du cycle de vie de votre système.
- Le *Dell License Manager User's Guide* (Guide d'utilisation de Dell License Manager) fournit des informations sur la gestion des licences de serveur de composant pour serveurs Dell 12G.
- Le *Glossaire* offre des informations sur la terminologie utilisée dans le présent document.

Accès aux documents à partir du site de support Dell

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

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

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

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

Obtention d'une assistance technique

Si à tout moment vous ne comprenez pas une des procédures décrites dans ce guide ou si le produit ne fonctionne pas comme prévu, des outils d'aide sont à votre disposition. Pour en savoir plus sur ces outils d'aide, consultez la section **Getting Help** (Obtention d'aide) du *Hardware Owner's Manual* (Manuel du propriétaire du matériel) de votre système.

En outre, une formation et une certification Dell Enterprise sont disponibles. Pour en savoir plus, voir **dell.com/training**. Il est possible que ce service ne soit pas offert dans certains emplacements.

Contacter Dell

REMARQUE : Dell fournit plusieurs options de service et de support en ligne et par téléphone. 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. La disponibilité des produits varie selon le pays et le produit. Il se peut que certains services ne soient pas disponibles dans votre région.

Pour prendre contact avec Dell pour des questions commerciales, de support technique ou de service clientèle :

1. Rendez-vous sur **dell.com/contactdell**.
2. Sélectionnez votre pays ou région depuis la carte du monde interactive.
   Les pays correspondant à la région sélectionnée s'affichent lorsque vous sélectionnez une région.
3. Sélectionnez la langue appropriée sous le pays de votre choix.
4. Sélectionnez votre secteur d'activités.
   La page de support principale pour le secteur d'activités sélectionné s'affichera.
5. Sélectionnez l'option appropriée en fonction de vos besoins.

REMARQUE : Si vous avez acheté un système Dell, l'on vous demandera peut-être de fournir le Numéro de service.

2

Configuration et administration

Dell OpenManage Server Administrator fournit de la sécurité en utilisant le contrôle de l'accès basé sur le rôle (RBAC), l'authentification et le cryptage pour les interfaces Web et de ligne de commande.

Contrôle des accès basé sur des rôles

RBAC gère la sécurité en déterminant quelles opérations doivent être exécutées par des personnes tenant un rôle particulier. Un ou plusieurs rôles sont attribués à chaque utilisateur et un ou plusieurs privilèges sont attribués à chaque rôle. Grâce RBAC, l'administration de la sécurité correspond à la structure d'une organisation.

Privilèges utilisateur

Server Administrator octroie différents droits d'accès en fonction des privilèges de groupe attribués à l'utilisateur. Les quatre niveaux de privilège utilisateur sont les suivants : Utilisateur, Utilisateur privilégié, Administrateur et Administrateur élevé.

Tableau 2. Privilèges utilisateur

Niveau de privilège de l'utilisateur	Type d'accès		Description
	Afficher	Gérer	
Utilisateur	Oui	Non	Les *utilisateurs* peuvent afficher la plupart des informations.
Utilisateur privilégié	Oui	Oui	Les *utilisateurs privilégiés* peuvent définir les valeurs des seuils d'avertissement et configurer les actions d'alerte qui doivent être effectuées lorsqu'un événement d'avertissement ou de panne se produit.
Administrateur	Oui	Oui	Les *administrateurs* peuvent configurer et réaliser des actions d'arrêt, configurer des actions de restauration automatique lorsque le système d'exploitation d'un système ne répond plus, et supprimer les journaux de matériel, d'événements et de commandes. Les administrateurs peuvent également configurer le système pour qu'il envoie des emails.
Administrateur élevé (Linux uniquement)	Oui	Oui	*Les administrateurs élevés* peuvent afficher et gérer les informations.

Niveaux de privilèges pour accéder aux services de Server Administrator

Le tableau suivant offre un récapitulatif des utilisateurs ayant les privilèges nécessaires pour accéder et gérer les services de Server Administrator.

Server Administrator accorde l'accès en lecture seule aux utilisateurs connectés avec des privilèges utilisateur, l'accès en lecture et en écriture aux utilisateurs connectés avec des droits d'utilisateur privilégié, et l'accès en lecture, en écriture et d'administrateur aux utilisateurs connectés avec des privilèges d'*administrateur* et d'*administrateur élevé*.

Tableau 3. Privilèges requis pour gérer les services de Server Administrator

Service	Niveau de privilège d'utilisateur requis	
	Afficher	Gérer
Instrumentation	Utilisateur, Utilisateur privilégié, Administrateur, Administrateur élevé	Utilisateur privilégié, Administrateur, Administrateur élevé
Accès à distance	Utilisateur, Utilisateur privilégié, Administrateur, Administrateur élevé	Administrateur, Administrateur élevé
Gestion du stockage	Utilisateur, Utilisateur privilégié, Administrateur, Administrateur élevé	Administrateur, Administrateur élevé

Authentification

Le schéma d'authentification de Server Administrator assure que des types d'adresse corrects sont attribués aux privilèges utilisateur corrects. En outre, lorsque l'interface de ligne de commande (CLI) est appelée, le schéma d'authentification de Server Administrator valide le contexte dans lequel le processus actuel s'exécute. Ce schéma d'authentification assure que toutes les fonctions de Server Administror, qu'elles soient utilisées depuis la page d'accueil de Server Administrator ou depuis la CLI, sont correctement authentifiées.

Authentification de Microsoft Windows

Sur les systèmes d'exploitation Microsoft Windows pris en charge, Server Administrator utilise Integrated Windows Authentication (précédemment appelée NTLM) pour effectuer l'authentification. Ce système d'authentification permet à la sécurité de Server Administrator d'être incorporée au schéma de sécurité d'ensemble de votre réseau.

Authentification de Red Hat Enterprise Linux et de SUSE Linux Enterprise Server

Sur des systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge, Server Administrator utilise différentes méthodes d'authentification sur la bibliothèque PAM (Pluggable Authentication Modules - Modules d'authentification enfichables). Les utilisateurs peuvent se connecter à Server Administrator localement ou à distance à l'aide de différents protocoles de gestion des comptes, tels que LDAP, NIS, Kerberos et Winbind.

Authentification de VMware ESX Server 4.X

VMware ESX Server utilise la structure PAM (Pluggable Authentication Modules - Modules d'authentification enfichable) pour l'authentification lorsque les utilisateurs accèdent à l'hôte ESX Server. La configuration PAM pour les services VMware stocke les chemins aux modules d'authentification et se trouve à l'emplacement suivant :**/etc/pam.d/vmware-authd**.

L'installation par défaut de ESX Server utilise l'authentification **/etc/passwd**, tout comme Linux, mais vous pouvez configurer le serveur ESX Server afin qu'il puisse utiliser un autre mécanisme d'authentification distribuée.

REMARQUE : Sur les systèmes exécutant le système d'exploitation VMware ESX Server 4.x, pour vous connecter à Server Administrator, tous les utilisateurs nécessitent des privilèges d'administrateur. Pour en savoir plus sur l'attribution des rôles, voir la documentation VMware.

Authentification de VMware ESXi Server 5.X

ESXi Server authentifie les utilisateurs accédant aux hôtes ESXi à l'aide du client vSphere/VI Client ou du kit de développement logiciel (SDK). L'installation par défaut de ESXi utilise une base de données de mots de passe locale pour l'authentification. Les transactions d'authentification ESXi avec Server Administrator interagissent également directement avec le processus **vmware-hostd**. Pour vous assurer que l'authentification fonctionne correctement pour votre site, effectuez des tâches de base telles que configurer les utilisateurs, les groupes, les permissions, les rôles et les attributs utilisateur, ajouter vos propres certificats et déterminer si vous souhaitez utiliser SSL.

REMARQUE : Sur les systèmes exécutant le système d'exploitation VMware ESXi Server 5.0, pour se connecter à Server Administrator, tous les utilisateurs nécessitent des privilèges d'administrateur. Pour en savoir plus sur l'attribution des rôles, voir la documentation VMware.

Cryptage

L'accès à Server Administrator s'effectue sur une connexion HTTPS sécurisée à l'aide de la technologie SSL (secure socket layer - couche de sockets sécurisée) pour assurer et protéger l'identité du système géré. JSSE (Java Secure Socket Extension - Extension de sockets sécurisée Java) est utilisée par les systèmes d'exploitation Microsoft Windows, Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge pour protéger les informations d'identification des utilisateurs et autres informations confidentielles transmises sur la connexion de socket lorsqu'un utilisateur accède à la page d'accueil **Server Administrator**.

Attribution des privilèges d'utilisateur

Pour assurer la sécurité des composants système critiques, attribuez des privilèges utilisateur à tous les utilisateurs du logiciel Dell OpenManage avant d'installer le logiciel Dell OpenManage. Les nouveaux utilisateurs peuvent se connecter au logiciel Dell OpenManage en utilisant leurs privilèges utilisateur de système d'exploitation.

PRÉCAUTION : Pour protéger l'accès aux composants critiques de votre système, attribuez un mot de passe à tous les comptes utilisateur pouvant accéder au logiciel Dell OpenManage. Les utilisateurs auxquels il n'a été attribué aucun mot de passe ne peuvent pas se connecter au logiciel Dell OpenManage sur un système exécutant Windows Server 2003 en raison de la conception du système d'exploitation.

PRÉCAUTION : Désactivez les comptes d'invités des systèmes d'exploitation Windows pris en charge pour protéger l'accès aux composants critiques de votre système. Il est recommandé de renommer les comptes d'invité de manière à ce que les scripts distants ne puissent pas activer les comptes à l'aide des noms de compte d'invités par défaut.

REMARQUE : Pour des instructions sur l'attribution de privilèges d'utilisateur pour chaque système d'exploitation pris en charge, consultez la documentation du système d'exploitation.

REMARQUE : Pour ajouter des utilisateurs au logiciel OpenManage, ajoutez de nouveaux utilisateurs au système d'exploitation. Vous n'avez pas à créer de nouveaux utilisateurs depuis le logiciel OpenManage.

Ajout d'utilisateurs à un domaine sur des systèmes d'exploitation Windows

REMARQUE : Microsoft Active Directory doit être installé sur votre système pour réaliser les procédures suivantes. Pour en savoir plus sur l'utilisation d'Active Directory, voir Using the Active Directory Login (Utilisation de l'ouverture de session Active Directory).

1. Naviguez vers **Control Panel** → **Administrative Tools** → **Active Directory Users and Computers** (Panneau de configurationÆ Outils d'administrationÆ Utilisateurs et ordinateurs Active Directory.).
2. Dans l'arborescence de la console, effectuez un clic droit sur **Users** (Utilisateurs) ou sur le conteneur auquel vous voulez ajouter le nouvel utilisateur et pointez sur **New** → **User** (Nouveau > Utilisateur).
3. Tapez les informations appropriées concernant le nom d'utilisateur dans la boîte de dialogue et cliquez sur **Next** (Suivant).
4. Cliquez sur **Next**, puis sur **Finish** (Terminer).
5. Double-cliquez sur l'icône représentant l'utilisateur que vous venez de créer.
6. Cliquez sur l'onglet **Member of** (Membre de).
7. Cliquez sur **Add** (Ajouter).
8. Sélectionnez le groupe approprié puis cliquez sur **Add** (Ajouter).
9. Cliquez sur **OK**, puis cliquez une deuxième fois sur **OK**.

   Les nouveaux utilisateurs peuvent ouvrir une session sur le logiciel Dell OpenManage avec les privilèges d'utilisateur de leur groupe et de leur domaine attribués.

Création d'utilisateurs Server Administrator sur les systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge

Des privilèges d'accès d'administrateur sont attribués à l'utilisateur connecté en tant qu'utilisateur racine. Pour créer des utilisateurs dotés de privilèges d'utilisateur et d'utilisateur privilégié, réalisez les étapes suivantes.

REMARQUE : Vous devez être connecté en tant qu'utilisateur `root` (racine) ou équivalent pour pouvoir effectuer ces procédures.

REMARQUE : Vous devez avoir installé l'utilitaire **useradd** sur votre système pour pouvoir effectuer ces procédures.

Création d'utilisateurs

REMARQUE : Pour des informations sur la création d'utilisateurs et de groupes d'utilisateurs, consultez la documentation de votre système d'exploitation.

Création d'utilisateurs avec des privilèges d'utilisateur

1. Exécutez la commande suivante depuis la ligne de commande : `useradd -d <home-directory> -g <group> <username>` où `<group>` (groupe) n'est pas le groupe `root` (racine).

   REMARQUE : Si `<group>` n'existe pas, vous devez le créer à l'aide de la commande **groupadd**.
2. Tapez `passwd <nom_d'utilisateur>` et appuyez sur <Entrée>.
3. Lorsque vous y êtes invité, entrez un mot de passe pour le nouvel utilisateur.

   REMARQUE : Vous devez attribuer un mot de passe à chaque compte d'utilisateur ayant accès à Server Administrator pour protéger l'accès aux composants critiques de votre système.

   Le nouvel utilisateur peut maintenant ouvrir une session sur Server Administrator avec les privilèges du groupe d'utilisateurs.

Création d'utilisateurs avec des privilèges d'utilisateur privilégié

1. Exécutez la commande suivante depuis la ligne de commande :`useradd -d <home-directory> -g <group> <username>`

   REMARQUE : Définissez `root` en tant que groupe principal.
2. Tapez `passwd <nom_d'utilisateur>` et appuyez sur <Entrée>.
3. Lorsque vous y êtes invité, entrez un mot de passe pour le nouvel utilisateur.

   REMARQUE : Vous devez attribuer un mot de passe à chaque compte d'utilisateur ayant accès à Server Administrator pour protéger l'accès aux composants critiques de votre système.

   Le nouvel utilisateur peut maintenant ouvrir une session sur Server Administrator avec les privilèges du groupe d'utilisateurs privilégiés.

Modification des privilèges d'utilisateur Server Administrator sur les systèmes d'exploitation Linux

REMARQUE : Vous devez être connecté en tant qu'utilisateur root ou équivalent pour pouvoir effectuer ces procédures.

1. Ouvrez le fichier **omarolemap** qui se trouve dans **/opt/dell/srvadmin/etc/omarolemap**.
2. Ajoutez ce qui suit au fichier : `<Nom_d'utilisateur>[Tab]<Nom_d'hôte>[Tab]<Droits>`

   Le tableau suivant répertorie les légendes pour l'ajout de la définition du rôle au fichier `omarolemap`

   Tableau 4. Légendes concernant l'ajout de la définition du rôle dans OpenManage Server Administrator

<Nom_d'utilisateur>	<Nom_d'hôte>	<Droits>
Nom d'utilisateur	Nom d'hôte	Administrateur
(+) Nom du groupe	Domaine	Utilisateur
Caractère générique (*)	Caractère générique (*)	Utilisateur
`[Tab] = \t (caractère de tabulation)`		

   Le tableau suivant répertorie les exemples pour l'ajout de la définition du rôle au fichier omarolemap.

   Tableau 5. Exemples pour l'ajout de la définition du rôle dans OpenManage Server Administrator

<Nom_d'utilisateur>	<Nom_d'hôte>	<Droits>
Bob	HôteA	Utilisateur privilégié
+ root	HôteB	Administrateur
+ root	HôteC	Administrateur
Bob	*.aus.amer.com	Utilisateur privilégié
Mike	192.168.2.3	Utilisateur privilégié

3. Enregistrez et fermez le fichier.

Meilleures pratiques lors de l'utilisation du fichier omarolemap

La liste suivante décrit les meilleures pratiques à prendre en compte lors de l'utilisation du fichier omarolemap :

- Ne supprimez pas les entrées par défaut suivantes dans le fichier **omarolemap**.

root	* Administrator (administrateur racine)
+root	* Poweruser (utilisateur avancé racine)
*	* User (Utilisateur racine)

- Ne modifiez pas les permissions ou le format du fichier **omarolemap.**
- N'utilisez pas l'adresse de retour de boucle pour *<Nom_d'hôte>*, par exemple : hôte local ou 127.0.0.1.
- Lorsque les services de connexion ont été redémarrés et que les modifications ne sont pas effectives pour le fichier **omarolemap**, consultez le journal des commandes pour prendre connaissance des erreurs.
- Lorsque le fichier **omarolemap** est copié d'un ordinateur à un autre, les permissions et les entrées du fichier doivent être revérifiées.
- Ajoutez le préfixe + au *Nom du groupe.*
- Server Administrator utilise les privilèges utilisateur par défaut du système d'exploitation si :
  - un utilisateur est dégradé dans le fichier **omarolemap**
  - il existe des saisies en double de noms d'utilisateurs et de groupes d'utilisateurs présentant en outre le même *<Nom_d'hôte>*
- `Espace` peut également être utilisé comme délimiteur pour les colonnes au lieu de `[Tab]`

Création d'utilisateurs Server Administrator pour VMware ESX 4.X, ESXi 4.X et ESXi 5.X

Pour ajouter un utilisateur au tableau répertoriant les utilisateurs :

1. Connectez-vous à l'hôte via vSphere Client.
2. Cliquez sur l'onglet **Users & Groups** (Utilisateurs et Groupes), puis cliquez sur **Users** (Utilisateurs).
3. Avec le bouton droit de la souris, cliquez n'importe où dans le tableau Utilisateurs, puis cliquez sur **Add** (Ajouter) pour ouvrir la boîte de dialogue **Add New User** (Ajouter un nouvel utilisateur).
4. Saisissez les ID d'ouverture de session et d'utilisateur numérique, le nom d'utilisateur et le mot de passe, en spécifiant que le nom d'utilisateur et l'ID d'utilisateur numérique sont facultatifs. Si vous ne spécifiez pas l'ID d'utilisateur numérique, le client vSphere attribue le prochain ID d'utilisateur numérique.
5. Pour permettre à un utilisateur d'accéder à l'hôte ESX/ESXi via un environnement de commande, sélectionnez **Grant shell access to this user** (Octroyer l'accès à l'environnement à cet utilisateur). Les utilisateurs qui accèdent au client vSphere n'ont pas besoin d'accéder à l'environnement.
6. Pour ajouter un utilisateur à un groupe, sélectionnez le nom du groupe dans le menu déroulant **Group** (Groupe) et cliquez sur **Add** (Ajouter).
7. Cliquez sur **OK**.

Désactivation de comptes d'invités et anonymes sur des systèmes d'exploitation Windows pris en charge

REMARQUE : Vous devez être connecté avec des privilèges d'administrateur pour pouvoir effectuer cette procédure.

1. Ouvrez la fenêtre **Computer Management** (Gestion de l'ordinateur).
2. Dans l'arborescence de la console, développez **Local Users and Groups** (Utilisateurs et groupes locaux), puis cliquez sur **Users** (Utilisateurs).
3. Double-cliquez sur le compte d'utilisateur dénommé **Guest** (Invité) ou **IUSR_system** (système_IUSR) pour afficher les propriétés de ces utilisateurs, ou effectuez un clic droit sur le compte d'utilisateur dénommé **Guest** ou **IUSR_***nom du système*, puis choisissez **Properties** (Propriétés).
4. Sélectionnez **Account is disabled** (Le compte est désactivé) et cliquez sur **OK**.

Un cercle rouge avec un X apparaît sur le nom d'utilisateur pour indiquer que le compte est désactivé.

Configuration de l'agent SNMP

Server Administrator prend en charge le protocole SMNP (protocole de gestion de réseau simple), un protocole de gestion des systèmes standard, sur tous les systèmes d'exploitation pris en charge. La prise en charge SNMP peut être installée ou non selon le système d'exploitation dont vous disposez et la façon dont celui-ci a été installé. Dans la plupart des cas, SNMP est installé lors de l'installation de votre système d'exploitation. Un protocole de gestion des systèmes standard installé et pris en charge, tel que SNMP, est nécessaire à l'installation de Server Administrator.

Vous pouvez configurer l'agent SNMP de manière à pouvoir modifier le nom de communauté, activer les opérations Set (de définition) et envoyer des interruptions à la station de gestion. Pour configurer votre agent SNMP de manière à ce qu'il interagisse correctement avec les applications de gestion telles que Dell OpenManage IT Assistant, réalisez les procédures décrites dans les sections suivantes.

REMARQUE : La configuration par défaut de l'agent SNMP inclut généralement un nom de communauté SNMP tel que « public ». Pour des raisons de sécurité, vous devez renommer les noms de communauté SNMP. Pour en savoir plus sur le renommage des noms de communauté SNMP, voir Modification du nom de communauté SNMP.

REMARQUE : Les opérations Set (de définition) SNMP sont désactivées par défaut dans Server Administrator version 5.2 ou ultérieure. Vous pouvez activer ou désactiver ces opérations depuis la page de configuration SNMP de Server Administrator sou Preferences (Préférences) ou à l'aide de l'interface de ligne de commande (CLI) de Server Administrator. Pour en savoir plus sur la CLI de Server Administrator, reportez-vous au *Dell OpenManage Server Administrator Command Line Interface Guide* (Guide de l'interface de ligne de commande de Server Administrateur) sur **dell.com/support/manuals**.

REMARQUE : Pour qu'IT Assistant puisse obtenir les informations de gestion depuis un système exécutant Server Administrateur, le nom de communauté qu'utilise IT Assistant doit correspondre à un nom de communauté utilisé par le système exécutant Server Administrator. Pour qu'IT Assistant puisse modifier des informations ou réaliser des actions sur un système exécutant Server Administrator, le nom de communauté qu'utilise IT Assistant doit correspondre à un nom de communauté autorisant les opérations Set (de définition) sur le système exécutant Server Administrateur. Pour qu'IT Assistant puisse recevoir des interruptions (des notifications d'événements asynchrones) provenant d'un système exécutant Server Administrator, le système exécutant Server Administrator doit être configuré pour l'envoi d'interruptions au système exécutant IT Assistant.

Les procédures suivantes fournissent des instructions détaillées pour configurer l'agent SNMP pour chaque système d'exploitation pris en charge :

- Configuration de l'agent SNMP pour les systèmes exécutant des systèmes d'exploitation Windows pris en charge
- Configuration de l'agent SNMP sur les systèmes fonctionnant sous un système d'exploitation Red Hat Enterprise Linux pris en charge
- Configuration de l'agent SNMP sur les systèmes fonctionnant sous des systèmes d'exploitation SUSE Linux Enterprise Server pris en charge
- Configuration de l'agent SNMP sur des systèmes fonctionnant sous les systèmes d'exploitation VMware ESX 4.X pris en charge sur les bases d'informations de gestion Proxy VMware
- Configuration de l'agent SNMP sur des systèmes exécutant les systèmes d'exploitation VMware ESXi 4.X et ESXi 5.X pris en charge

Configuration de l'agent SNMP sur les systèmes exécutant des systèmes d'exploitation Windows pris en charge

Server Administrator utilise les services SNMP fournis par l'agent SNMP Windows. Vous pouvez configurer l'agent SNMP pour modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à la station de gestion. Pour configurer l'agent SNMP pour qu'il interagisse correctement avec les applications de gestion telles qu'IT Assistant, réalisez les procédures décrites dans les sections suivantes.

REMARQUE : Pour des détails supplémentaires sur la configuration SNMP, consultez la documentation de votre système d'exploitation.

Activation de l'accès SNMP sur des hôtes distants (Windows Server 2003 uniquement)

Windows Server 2003, par défaut, n'accepte pas de paquets SNMP provenant d'hôtes distants. Dans le cas de systèmes exécutant Windows Server 2003, vous devez configurer le service SNMP de manière à ce qu'il accepte les paquets SNMP provenant d'hôtes distants si vous comptez gérer le système à l'aide d'applications de gestion SNMP provenant d'hôtes distants.

Pour activer un système exécutant Windows Server 2003 afin de recevoir des paquets SNMP provenant d'un hôte distant, procédez comme suit :

1. Ouvrez la fenêtre **Computer Management** (Gestion de l'ordinateur).
2. Développez l'icône **Computer Management** dans la fenêtre, si nécessaire.
3. Développez l'icône **Services and Applications** (Services et applications) et cliquez sur **Services**.
4. Faites défiler la liste des services jusqu'à ce que vous trouviez **SNMP Service** (Service SNMP), effectuez un clic droit sur **SNMP Service**, puis cliquez sur **Properties** (Propriétés).

   La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
5. Cliquez sur l'onglet **Security** (Sécurité).
6. Sélectionnez **Accept SNMP packets from any host** (Accepter les paquets SNMP provenant de n'importe quel hôte) ou ajoutez l'hôte distant à la liste **Accept SNMP packets from these hosts** (Accepter les paquets SNMP provenant de ces hôtes).

Modification du nom de communauté SNMP

La configuration des noms de communauté SNMP détermine quels systèmes sont capables de gérer votre système via SNMP. Les noms de communauté SNMP utilisés par les applications de gestion doivent correspondre à un nom de communauté SNMP configuré sur le système exécutant Server Administrator de manière à ce que les applications de gestion puissent obtenir des informations de gestion depuis Server Administrator.

1. Ouvrez la fenêtre **Computer Management** (Gestion de l'ordinateur).
2. Développez l'icône **Computer Management** dans la fenêtre, si nécessaire.
3. Développez l'icône **Services and Applications** (Services et applications) et cliquez sur **Services**.
4. Faites défiler la liste des services jusqu'à ce que vous trouviez **SNMP Service** (Service SNMP), effectuez un clic droit sur **SNMP Service**, puis cliquez sur **Properties** (Propriétés).

   La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
5. Cliquez sur l'onglet **Security** (Sécurité) pour ajouter ou modifier un nom de communauté.

   Pour ajouter un nom de communauté :

   a. Cliquez sur **Add** (Ajouter) sous la liste **Accepted Community Names** (Noms de communs acceptés).

      La fenêtre **SNMP Service Configuration** (Configuration du service SNMP) apparaît.

   b. Saisissez le nom de communauté d'un système qui peut gérer votre système (public par défaut) dans la zone de texte **Nom de communauté** et cliquez sur **Add** (Ajouter).

      La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.

   Pour modifier un nom de communauté :

   a. Sélectionnez un nom de communauté dans la liste **Accepted Community Names** (Noms de communauté acceptés) et cliquez sur **Edit** (Modifier).

      La fenêtre **SNMP Service Configuration** (Configuration du service SNMP) apparaît.

   b. Modifiez le nom de communauté dans la boîte de dialogue **Community Name** (Nom de communauté), puis cliquez sur **OK** .

      La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
6. Cliquez sur **OK** pour enregistrer les modifications.

Activation des opérations Set SNMP

Les opérations Set SNMP doivent être activées sur le système Server Administrator pour que vous puissiez modifier les attributs de Server Administrator avec IT Assistant.

1. Ouvrez la fenêtre **Computer Management** (Gestion de l'ordinateur).
2. Développez l'icône **Computer Management** dans la fenêtre, si nécessaire.
3. Développez l'icône **Services and Applications** (Services et applications) et cliquez sur **Services**.
4. Faites défiler la liste des services jusqu'à ce que vous trouviez **SNMP Service** (Service SNMP), effectuez un clic droit sur **SNMP Service**, puis cliquez sur **Properties** (Propriétés).

   La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
5. Cliquez sur l'onglet **Security** (Sécurité) pour modifier les droits d'accès d'une communauté.
6. Sélectionnez un nom de communauté dans la liste **Accepted Community Names** (Noms de communauté acceptés) et cliquez sur **Edit** (Modifier).

   La fenêtre **SNMP Service Configuration** (Configuration du service SNMP) apparaît.
7. Définissez les **Community rights** (Droits de communauté) sur **READ WRITE or READ CREATE** (LECTURE-ÉCRITURE OU LECTURE-CRÉATION), puis cliquez sur **OK**.

   La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
8. Cliquez sur **OK** pour enregistrer les modifications.

Configuration de votre système pour envoyer des interruptions SNMP à une station de gestion

Server Administrator génère des interruptions SNMP en réponse aux modifications de la condition des capteurs et d'autres paramètres surveillés. Vous devez configurer une ou plusieurs destinations d'interruption sur le système exécutant Server Administrator afin d'envoyer des interruptions SNMP à une station de gestion.

1. Ouvrez la fenêtre **Computer Management** (Gestion de l'ordinateur).
2. Développez l'icône **Computer Management** dans la fenêtre, si nécessaire.
3. Développez l'icône **Services and Applications** (Services et applications) et cliquez sur **Services**.
4. Faites défiler la liste des services jusqu'à ce que vous trouviez **SNMP Service** (Service SNMP), effectuez un clic droit sur **SNMP Service**, puis cliquez sur **Propriétés**.

   La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
5. Cliquez sur l'onglet **Traps** (Interruptions) pour ajouter une communauté d'interruptions ou pour ajouter une destination d'interruption à une communauté d'interruption.
   a. Pour ajouter une communauté d'interruptions, tapez le nom de la communauté dans la boîte **Community Name** (Nom de la communauté) et cliquez sur **Add to list** (Ajouter à la liste), en regard de la boîte **Community Name**.
   b. Pour ajouter une destination d'interruption pour une communauté d'interruptions, sélectionnez le nom de communauté dans la boîte déroulante **Community Name** et cliquez sur **Add** (Ajouter) sous la boîte **Trap Destinations** (Destinations d'interruption).

      La fenêtre **SNMP Service Configuration** (Configuration du service SNMP) apparaît.
   c. Dans les boîtes **Host name** (Nom d'hôte), **IP or IPX address** (Adresse IP ou IPX), saisissez la destination d'interruption, puis cliquez sur **Add**.

      La fenêtre **SNMP Service Properties** (Propriétés de service SNMP) apparaît.
6. Cliquez sur **OK** pour enregistrer les modifications.

Configuration de l'agent SNMP sur les systèmes exécutant un système d'exploitation Red Hat Enterprise Linux pris en charge

Server Administrator utilise les services SNMP fournis par l'agent SNMP Windows **net-snmp**. Vous pouvez configurer l'agent SNMP pour modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à la station de gestion. Pour configurer l'agent SNMP pour qu'il interagisse correctement avec les applications de gestion telles qu'IT Assistant, réalisez les procédures décrites dans les sections suivantes.

REMARQUE : Pour des détails supplémentaires sur la configuration SNMP, consultez la documentation de votre système d'exploitation.

Configuration du contrôle d'accès de l'agent SNMP

La branche MIB (management information base - base d'informations de gestion) mise en œuvre par Server Administrator est identifiée par son OID (identifiant d'objet) 1.3.6.1.4.1.674. Les applications de gestion doivent avoir accès à cette branche de l'arborescence MIB pour gérer les systèmes exécutant Server Administrator.

Dans le cas des systèmes d'exploitation Red Hat Enterprise Linux et VMware ESXi 4.0, la configuration par défaut de l'agent SNMP donne un accès en lecture seule à la communauté *public* uniquement à la branche *system* (système) MIB-II (identifiée par l'OID 1.3.6.1.2.1.1) de l'arborescence MIB. Cette configuration ne permet pas aux applications de gestion d'obtenir ou de modifier Server Administrator ou d'autres informations de gestion des systèmes hors de la branche *system* MIB-II.

Actions d'installation de l'agent SNMP de Server Administrator

Si Server Administrator détecte la configuration SNMP par défaut pendant l'installation, il tente de modifier la configuration de l'agent SNMP pour fournir un accès en lecture seule à l'intégralité de l'arborescence MIB (base d'informations de gestion) de la communauté « public ». Server Administrator modifie le fichier de configuration de l'agent SNMP **/etc/snm, p/snmpd.conf** en :

- créant une vue de l'intégralité de l'arborescence MIB en ajoutant la ligne suivante (si celle-ci n'existe pas déjà) : `view all included`
- modifiant la ligne d'accès par défaut pour fournir un accès en lecture seule à l'intégralité de l'arborescence MIB (base d'informations de gestion) de la communauté « public ». Server Administrator cherche la ligne suivante : `access notConfigGroup "" any noauth exact systemview none none`
- Si Server Administrator trouve la ligne susmentionnée, il la modifie comme suit : `access notConfigGroup "" any noauth exact all none none`

  REMARQUE : Afin que Server Administrator puisse modifier la configuration de l'agent SNMP pour fournir un accès approprié aux données de gestion de systèmes, il est recommandé que toute autre modification de la configuration de l'agent SNMP soit effectuée après l'installation de Server Administrator.

Le protocole SNMP de Server Administrator communique avec l'agent SNMP à l'aide du protocole SNMP Multiplexing (SMUX) . Lorsque le protocole SNMP de Server Administrator se connecte à l'agent SNMP, il envoie un identifiant d'objet à l'agent SNMP pour s'identifier auprès de ce dernier en tant qu'homologue SMUX. Étant donné que cet identifiant d'objet doit être configuré avec l'agent SNMP, Server Administrator ajoute la ligne suivante au fichier de configuration de l'agent SNMP pendant l'installation (si celle-ci n'existe pas déjà) : **/etc/snmp/snmpd.conf** :

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Modification du nom de communauté SNMP

La configuration des noms de communauté SNMP détermine quels systèmes sont capables de gérer votre système via SNMP. Les noms de communauté SNMP utilisés par les applications de gestion doivent correspondre à un nom de communauté SNMP configuré sur le système exécutant Server Administrator de manière à ce que les applications de gestion puissent obtenir des informations de gestion depuis Server Administrator.
Pour modifier le nom de communauté SNMP utilisé pour récupérer les informations de gestion depuis un système exécutant Server Administrator :

1. Ouvrez le fichier de configuration de l'agent SNMP, **/etc/snmp/snmpd.conf**.
2. Trouvez la ligne suivante : `com2sec publicsec default public` ou `com2sec notConfigUser default public`.

   REMARQUE : Pour IPv6, trouvez la ligne `com2sec6 notConfigUser default public`. Ajoutez également le texte suivant au fichier : `agentaddress udp6:161`.
3. Modifiez cette ligne en remplaçant `public` par le nouveau nom de communauté SNMP. Une fois modifiée, la nouvelle ligne devrait être comme suit : `com2sec publicsec default community_name` ou `com2sec notConfigUser default community_name`.

4. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant `service snmpd restart`.

Activation des opérations Set SNMP

Les opérations Set SNMP doivent être activées sur le système exécutant Server Administrator pour pouvoir modifier les attributs de Server Administrator à l'aide d'IT Assistant.

Pour activer les opérations Set SNMP sur le système qui exécute Server Administrator, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Trouvez la ligne `access publicgroup "" any noauth exact all none none` ou la ligne `access notConfigGroup "" any noauth exact all none none`.
2. Modifiez cette dernière, en remplaçant le premier `none` (aucun) par `all` (tous). Une fois modifiée, la nouvelle ligne devrait être comme suit : `access publicgroup "" any noauth exact all all none` ou `access notConfigGroup "" any noauth exact all all none`.
3. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : `service snmpd restart`.

Configuration de votre système pour envoyer des interruptions à une station de gestion

Server Administrator génère des interruptions SNMP en réponse aux modifications de l'état des capteurs et autres paramètres surveillés. Vous devez configurer une ou plusieurs destinations d'interruption sur le système exécutant Server Administrator afin d'envoyer des interruptions SNMP à une station de gestion.

Pour configurer le système exécutant Server Administrator pour qu'il envoie des interruptions à une station de gestion, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Ajoutez la ligne suivante au fichier : `trapsink IP_address community_name`, où `IP_address` correspond à l'adresse IP de la station de gestion et `community_name` est le nom de la communauté SNMP.
2. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : `service snmpd restart`.

Configuration de l'agent SNMP sur les systèmes exécutant des systèmes d'exploitation SUSE Linux Enterprise Server pris en charge

Server Administrator utilise les services SNMP fournis par l'agent net-snmp. Vous pouvez configurer l'agent SNMP pour activer l'accès SNMP depuis un hôte distant, modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à la station de gestion. Pour configurer votre agent SNMP pour qu'il interagisse correctement avec les applications de gestion telles qu'IT Assistant, réalisez les procédures décrites dans les sections suivantes.

REMARQUE : Pour obtenir des détails supplémentaires sur la configuration SNMP, reportez-vous à la documentation du système d'exploitation.

Actions d'installation SNMP de Server Administrator

Le protocole SNMP de Server Administrator communique avec l'agent SNMP à l'aide du protocole SMUX. Lorsque le protocole SNMP de Server Administrator se connecte à l'agent SNMP, il envoie un identifiant d'objet à l'agent SNMP pour s'identifier auprès de ce dernier en tant qu'homologue SMUX. Étant donné que cet identifiant d'objet doit être configuré avec l'agent SNMP, Server Administrator ajoute la ligne suivante au fichier de configuration de l'agent SNMP pendant l'installation (si celle-ci n'existe pas déjà) : **/etc/snmp/snmpd.conf** :

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Activation de l'accès SNMP à partir d'hôtes distants

La configuration par défaut de l'agent SNMP sur les systèmes d'exploitation SUSE Linux Enterprise Server fournit un accès en lecture seule à l'intégralité de l'arborescence MIB (base d'information de gestion) de la communauté « public » depuis l'hôte local uniquement. Cette configuration ne permet pas aux applications de gestion SNMP telles qu'IT Assistant de s'exécuter sur d'autres hôtes pour découvrir et gérer correctement les systèmes Server

Administrator. Si Server Administrator détecte cette configuration pendant l'installation, il enregistre un message dans le fichier journal du système d'exploitation, **/var/log/messages**, pour indiquer que l'accès SNMP est limité à l'hôte local. Vous devez configurer l'agent SNMP pour activer l'accès SNMP à partir d'hôtes distants si vous comptez gérer le système à l'aide d'applications de gestion SNMP d'hôtes distants.

REMARQUE : Pour des raisons de sécurité, il est conseillé de restreindre l'accès SNMP à des hôtes distants spécifiques, si possible.

Pour activer l'accès SNMP à partir d'un hôte distant spécifique à un système exécutant Server Administrator, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Trouvez la ligne `rocommunity public 127.0.0.1`.
2. Modifiez ou copiez cette ligne, en remplaçant 127.0.0.1 par l'adresse IP de l'hôte distant. Une fois modifiée, la nouvelle ligne devrait être comme suit : `rocommunity public IP_address`.

   REMARQUE : Vous pouvez activer l'accès SNMP à partir de plusieurs hôtes distants spécifiques en ajoutant une directive `rocommunity` pour chaque hôte distant.
3. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : `/etc/init.d/snmpd restart`.

   Pour activer l'accès SNMP à partir de tous les hôtes distants à un système exécutant Server Administrator, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :
4. Trouvez la ligne `rocommunity public 127.0.0.1`.
5. Modifiez cette ligne en supprimant 127.0.0.1. Une fois modifiée, la nouvelle ligne devrait être comme suit : `rocommunity public`.
6. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : `/etc/init.d/snmpd restart`.

Modification du nom de communauté SNMP

La configuration des noms de communauté SNMP détermine quelles stations de gestion sont capables de gérer votre système via SNMP. Les noms de communauté SNMP utilisés par les applications de gestion doivent correspondre au nom de communauté SNMP configuré sur le système exécutant Server Administrator de manière à ce que les applications de gestion puissent obtenir des informations de gestion depuis Server Administrator.

Pour modifier le nom de communauté SNMP par défaut utilisé pour récupérer les informations de gestion depuis un système exécutant Server Administrator :

1. Ouvrez le fichier de configuration de l'agent SNMP, **/etc/snmp/snmpd.conf**.
2. Trouvez la ligne : `rocommunity public 127.0.0.1.`
3. Modifiez cette ligne en remplaçant `public` par le nouveau nom de communauté SNMP. Une fois modifiée, la nouvelle ligne devrait être comme suit : `rocommunity community_name 127.0.0.1.`
4. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : **/etc/init.d/snmpd restart**.

Activation des opérations Set SNMP

Les opérations Set SNMP doivent être activées sur le système exécutant Server Administrator afin de modifier les attributs de Server Administrator à l'aide d'IT Assistant. Pour activer l'arrêt à distance d'un système depuis IT Assistant, les opérations Set SNMP doivent être activées.

REMARQUE : Le redémarrage de votre système pour la fonctionnalité de gestion des modifications ne nécessite pas les opérations set SNMP.

Pour activer les opérations Set SNMP sur un système exécutant Server Administrator :

1. Ouvrez le fichier de configuration de l'agent SNMP, **/etc/snmp/snmpd.conf**.
2. Trouvez la ligne `rocommunity public 127.0.0.1`.

3. Modifiez cette ligne en remplaçant `rocommunity` par `rwcommunity`. Une fois modifiée, la nouvelle ligne devrait être la suivante : `rwcommunity public 127.0.0.1`.
4. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : **/etc/init.d/snmpd restart**.

Configuration de l'agent SNMP sur des systèmes exécutant des systèmes d'exploitation VMware ESX 4.X pris en charge sur les bases d'informations de gestion Proxy VMware

Le serveur ESX 4.X peut être géré via un port par défaut unique 162 à l'aide du protocole SNMP. Pour ce faire, `snmpd` est configuré pour utiliser le port par défaut 162 et `vmwarehostd` est configuré pour utilisé un port différent (non utilisé), par exemple, 167. Toute demande SNMP sur la branche MIB VMware est réacheminée vers le **vmware-hostd** à l'aide de la fonction proxy du démon **snmpd**.

Le fichier de configuration SNMP VMWware peut être modifié manuellement sur le serveur ESX ou en exécutant la commande RCLI (Remote Command-Line Interface) VMware, `vicfg-snmp`, depuis un système distant (Windows ou Linux). Les outils RCLI sont téléchargeables depuis le site Web VMware à l'adresse suivante **vmware.com/download/vi/drivers_tools.html.**

Pour configurer l'agent SNMP :

1. Modifiez le fichier de configuration SNMP VMware, **/etc/vmware/snmp.xml**, manuellement ou en exécutant les commandes suivantes `vicfg-snmp` pour modifier les paramètres de configuration SNMP (lesquels incluent le port d'écoute SNMP, la chaîne de communauté, l'adresse IP/le port cible des interruptions et le nom de communauté d'interruptions) puis activez le service SNMP VMware.
   a. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -c <community name> -p X -t <Destination_IP_Address> @162/ <community name>`

      où représente un port non utilisé. Pour trouver un port non utilisé, consultez le fichier **/etc/services** pour l'attribution des ports pour les services système définis. En outre, pour vous assurer que le port sélectionné n'est pas actuellement utilisé par une application ou un service, exécutez la commande suivante sur le serveur ESX : `netstat –a command`

      REMARQUE : Plusieurs adresses IP peuvent être entrées en utilisant une liste séparée par des virgules.

      Pour activer le service SNMP VMWare, exécutez la commande suivante :
   b. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> - E`

      Pour afficher les paramètres de configuration, exécutez la commande suivante :
   c. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -s`

      Voici un exemple d'un fichier de configuration une fois modifié :

```
<?xml version="1.0">
<config>
<paramètres_snmp>
<activer>true</activer>
<communautés>public</communautés>
<cibles>143.166.152.248@162/public</cibles>
<port>167</port>
</paramètres_snmp>
</config>
```

2. Arrêtez le service SNMP s'il est déjà en cours d'exécution sur votre système en entrant la commande suivante : `service snmpd stop`
3. Ajoutez la ligne suivante à la fin du nom du fichier **/etc/snmp/snmpd.conf** : `proxy -v 1 -c public udp: 127.0.0.1:X .1.3.6.1.4.1.6876`

Où X représente le port inutilisé spécifié ci-dessus, tout en configurant SNMP.

4. Configurez la destination de l'interruption à l'aide de la commande suivante : `<Adresse_IP_de_destination> <nom_de_communauté>`

   La spécification trapsink est obligatoire pour envoyer les interruptions définies dans les bases d'informations de gestion propriétaires.

5. Redémarrez le service mgmt-vmware à l'aide de la commande suivante : `service mgmt-vmware restart`
6. Redémarrez le service snmpd à l'aide de la commande suivante : `service snmpd start`

   REMARQUE : Si srvadmin est installé et les services sont déjà en cours d'exécution, redémarrez ces derniers car ils dépendent du service **snmpd**.

7. Exécutez la commande suivante afin que le démon snmpd démarre lors de chaque redémarrage : `chkconfig snmpd on`
8. Exécutez la commande suivante pour garantir que les ports SNMP sont ouverts avant d'envoyer les interruptions à la station de gestion : `esxcfg-firewall -e snmpd`.

Configuration de l'agent SNMP sur des systèmes exécutant les systèmes d'exploitation VMware ESXi 4.X et ESXi 5.X pris en charge

Server Administrator prend en charge les interruptions SNMP sur VMware ESXi 4.X et ESXi 5.X. Si seule une licence autonome est présente, la configuration SNMP échoue sur les systèmes d'exploitation VMware ESXi. Server Administrator ne prend pas en charge les opérations Get et Set SNMP sur VMWare ESXi 4.X et ESXi 5.X, car la prise en charge SNMP requise n'est pas disponible. L'interface de ligne de commande (CLI) VMware vSphere sert à configurer les systèmes exécutant VMware ESXi 4.X et ESXi 5.X pour qu'ils envoient des interruptions SNMP à la station de gestion.

REMARQUE : Pour en savoir plus sur la CLI VMware vSphere, voir **vmware.com/support**.

Configuration de votre système pour envoyer des interruptions à une station de gestion

Server Administrator génère des interruptions SNMP en réponse aux modifications de l'état des capteurs et autres paramètres surveillés. Vous devez configurer une ou plusieurs destinations d'interruption sur le système exécutant Server Administrator afin d'envoyer des interruptions SNMP à une station de gestion.

Configurez le système ESXi exécutant Server Administrator pour qu'il envoie des interruptions à une station de gestion :

1. Installez la CLI VMware vSphere.
2. Ouvrez une invite de commande sur le système où la CLI VMware vSphere est installée.
3. Modifiez le répertoire dans lequel la CLI VMware vSphere est installée. L'emplacement par défaut sous Linux est **/usr/bin**. L'emplacement par défaut sous Windows est **C:\Program Files\VMware\VMware vSphere CLI\bin**.
4. Exécutez la commande suivante : `vicfg-snmp.pl --server <serveur> --username <nom_d'utilisateur> --password <mot_de_passe> -c <communauté> -t <nom_d'hôte> @162/<communauté>`

   où `<serveur>` correspond au nom d'hôte ou à l'adresse IP du système ESXi, `<nom_d'utilisateur>` correspond à l'utilisateur sur le système ESXi, `<communauté>` correspond au nom de communauté SNMP et `<nom_d'hôte>` correspond au nom d'hôte ou à l'adresse IP de la station de gestion.

   REMARQUE : L'extension .pl n'est pas requise sur Linux.

   REMARQUE : Si vous ne spécifiez pas de nom d'utilisateur et de mot de passe, vous êtes invité à le faire.

La configuration des interruptions SNMP prend immédiatement effet sans avoir besoin de redémarrer les services.

Configuration du pare-feu sur les systèmes exécutant les systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge

Si vous activez la sécurité du pare-feu alors que l'installation de Red Hat Enterprise Linux/SUSE Linux est en cours, le port SNMP de toutes les interfaces réseau externes est fermé par défaut. Pour autoriser les applications de gestion SNMP telles qu'IT Assistant à découvrir et obtenir des informations depuis Server Administrator, le port SNMP d'au moins une interface réseau externe doit être ouvert. Si Server Administrator détecte qu'aucun port SNMP d'interface réseau externe n'est ouvert dans le pare-feu, il affiche un message d'avertissement et enregistre un message dans le journal système.

Vous pouvez ouvrir le port SNMP en désactivant le pare-feu, ouvrant ainsi l'intégralité de l'interface réseau dans le pare-feu, ou en ouvrant le port SNMP d'une interface réseau externe au moins dans le pare-feu. Vous pouvez réaliser cette action avant ou après le démarrage de Server Administrator.

Pour ouvrir le port SNMP sur Red Hat Enterprise Linux à l'aide d'une des méthodes décrites précédemment, procédez comme suit :

1. À l'invite de commande Red Hat Enterprise Linux, tapez `setup` et appuyez sur <Entrée> pour lancer l'utilitaire de configuration du mode textuel.

   REMARQUE : Cette commande n'est disponible que si vous avez effectué une installation par défaut du système d'exploitation.

   Le menu **Choose a Tool** (Choisir un outil) apparaît.
2. Sélectionnez **Firewall Configuration** (Configuration du pare-feu) en utilisant la flèche vers le bas et appuyez sur <Entrée>.

   L'écran **Firewall Configuration** apparaît.
3. Appuyez sur <Tab> pour sélectionner **Security Level** (Niveau de sécurité), puis appuyez sur la barre d'espace pour sélectionner le niveau de sécurité que vous souhaitez configurer. Le **Security Level** (Niveau de sécurité) sélectionné est indiqué par un astérisque.

   REMARQUE : Pour en savoir plus sur les niveaux de sécurité du pare-feu, appuyez sur la touche <F1>. Le numéro du port SNMP par défaut est 161. Si vous utilisez l'interface d'utilisateur graphique X Window System, le fait d'appuyer sur la touche <F1> ne vous permettra pas nécessairement d'obtenir des informations sur les niveaux de sécurité du pare-feu de versions de Red Hat Enterprise Linux plus récentes.

   a. Pour désactiver le pare-feu, sélectionnez **No Firewall** (Pas de pare-feu) ou **Disabled** (Désactivé)et passez à l'étape 7.
   b. Pour ouvrir toute l'interface réseau ou le port SNMP, sélectionnez **High, Medium** (Élevé, Moyen) ou **Enabled** (Activé) et passez à l'étape 4.
4. Appuyez sur <Tab> pour accéder à la section Customize (Personnaliser), puis appuyez sur <Entrée>.

   L'écran **Firewall Configuration-Customize** (Configuration du pare-feu - Personnaliser) apparaît.
5. Sélectionnez s'il faut ouvrir toute l'interface réseau ou seulement le port SNMP sur toutes les interfaces réseau.
   a. Pour ouvrir toute l'interface réseau, appuyez sur <Tab> pour aller aux Trusted Devices (Périphériques de confiance), puis appuyez sur la barre d'espace. Un astérisque se trouve dans la boîte à gauche du nom du périphérique pour indiquer que toute l'interface est ouverte.
   b. Pour ouvrir le port SNMP sur toutes les interfaces réseau, appuyez sur <Tab> pour sélectionner Other ports (Autres ports) et saisissez `snmp:udp`.
6. Appuyez sur **<Tab>** pour sélectionner **OK**, puis appuyez sur **<Entrée>**.

   L'écran **Firewall Configuration** apparaît.
7. Appuyez sur **<Tab>** pour sélectionner **OK**, puis appuyez sur **<Entrée>**.

   Le menu **Choose a Tool** (Choisir un outil) apparaît.
8. Appuyez sur **<Tab>** pour sélectionner **Quit** (Quitter), puis appuyez sur **<Entrée>**.

Configuration du pare-feu

Pour ouvrir le port SNMP sur SUSE Linux Enterprise Server :

1. Configurer le pare-feu SuSEfirewall2 en exécutant le commande suivante sur une console : `a.# yast2 firewall`
2. Utilisez les touches fléchées pour naviguer vers **Allowed Services** (Services autorisés).
3. Appuyez sur les touches <Alt><d> pour ouvrir la boîte de dialogue **Additional Allowed Ports** (Ports autorisés supplémentaires).
4. Appuyez sur les touches <Alt><T> pour déplacer le curseur dans la zone de texte **Ports TCP**.
5. Entrez **snmp** dans la zone de texte.
6. Appuyez sur <Alt><O> <Alt><N> pour passer à l'écran suivant.
7. Appuyez sur les touches <Alt><A> pour accepter et appliquer les modifications.

3

Utilisation de Server Administrator

Pour ouvrir une session Server Administrator, double-cliquez sur l'icône **Dell OpenManage Server Administrator** sur votre bureau.

L'écran **Server Administrator Log in** (Ouverture de session Server Administrator) s'affiche. Le port par défaut pour Dell OpenManage Server Administrator est 1311. Vous pouvez modifier le port, le cas échéant. Pour des instructions sur la configuration de vos préférences système, voir Dell Systems Management Server Administration (Administration du serveur de gestion des systèmes Dell).

REMARQUE : Les serveurs exécutant XenServer 6.0 peuvent être gérés à l'aide de l'interface CLI ou d'un serveur Web central installé sur une machine distincte.

Ouverture et fermeture de session

OpenManage Server Administrator fournit les types d'ouverture de session suivants :

- Ouverture d'une session Server Administrator sur le système local
- Connexion au système géré de Server Administrator — Utilisation de l'icône de bureau
- Connexion au système géré de Server Administrator — Utilisation du navigateur Web
- Ouverture d'une session Central Web Server

Ouverture d'une session Server Administrator sur le système local

Cette ouverture de session est disponible uniquement si les composants Server Instrumentation et Server Administrator Web Server sont installés sur le système local.

Cette option est disponible pour les serveurs exécutant XenServer 6.0

Pour ouvrir une session Server Administrator sur un système local :

1. Tapez votre **Nom d'utilisateur** et votre **Mot de passe** préattribués dans les champs appropriés de la fenêtre **Log in** (Ouverture d'une session) de Systems Management.

   Si vous accédez à Server Administrator à partir d'un domaine défini, vous devez également spécifier le nom de domaine approprié.
2. Cochez la case **Active Directory Login** (Ouverture de session Active Directory) pour vous connecter avec Microsoft Active Directory. Voir Utilisez de l'ouverture de session Active Directory.
3. Cliquez sur **Submit** (Soumettre).

Pour mettre fin à votre session Server Administrator, cliquez sur le bouton **Log Out** (Fermer la session), dans le coin supérieur droit de chaque page d'accueil de **Server Administrator**.

REMARQUE : Pour en savoir plus sur la configuration d'Active Directory sur les systèmes utilisant la CLI, voir le *Dell OpenManage Management Station Software Installation Guide* (Guide d'installation du logiciel OpenManage Management Station) à l'adresse **dell.com/support/manuals**.

Connexion au système géré de Server Administrator — Utilisation de l'icône de bureau

Ce type de connexion est uniquement disponible si le composant Server Administrator Web Server est installé sur le système. Pour se connecter à Server Administrator afin de gérer un système distant :

1. Double-cliquez sur l'icône**Dell OpenManage Server Administrator** qui se trouve sur votre bureau.
2. Tapez l'adresse IP du système géré, le nom du système ou le nom de domaine complet (FQDN).

   REMARQUE : Si vous avez saisi le nom du système ou le FQDN, l'hôte Dell OpenManage Server Administrator Web Server convertit le nom du système ou le FQDN en l'adresse IP du système géré. Vous pouvez également saisir le numéro de port du système géré. Par exemple, Hostname:Port number (Nom d'hôte:Numéro de port), ou IP address:Port number (Adresse IP:Numéro de port). Si vous vous connectez à un nœud géré Citrix XenServer 6.0, utilisez le port 5986 au format Hostname:Port number (Nom d'hôte:Numéro de port), ou IP address:Port number (Adresse IP:Numéro de port).
3. Si vous utilisez une connexion Intranet, sélectionnez **Ignore Certificate Warnings** (Ignorer les avertissements de certificat).
4. Sélectionnez **Active Directory Login** (Ouverture de session Active Directory) pour vous connecter avec l'authentification Microsoft Active Directory. Si le logiciel Active Directory ne sert pas à contrôler l'accès à votre réseau, ne sélectionnez pas **Active Directory Login**. Voir Utilisation de la connexion Active Directory.
5. Cliquez sur **Submit** (Soumettre).

Connexion au système géré de Server Administrator — Utilisation du navigateur Web

REMARQUE : Vous devez disposer de droits pré attribués pour vous connecter à Server Administrator. Voir Configuration et administration pour des instructions pour configurer de nouveaux utilisateurs.

1. Ouvrez le navigateur Web.
2. Dans le champ d'adresse, tapez l'un des éléments suivants :
   - `https://hostname:1311`, où hostname (nom d'hôte) est le nom attribué au système géré et 1311 le numéro de port par défaut
   - `https://IP address:1311`, où IP address (Adresse IP) est l'adresse IP du système géré et 1311 est le numéro de port par défaut.

   REMARQUE : Assurez-vous de bien saisir `https://` (et non `http://`) dans le champ d'adresse.
3. Appuyez sur <Entrée>.

Ouverture d'une session Central Web Server

Cette ouverture de session est disponible uniquement si le composant Server Administrator Web Server est installé sur le système. Utilisez cette ouverture de session pour gérer OpenManage Server Administrator Central Web Server :

1. Double-cliquez sur l'icône **Dell OpenManage Server Administrator** de votre bureau. La page de connexion à distance s'affiche.

   PRÉCAUTION : L'écran d'ouverture de session affiche une case à cocher Ignore certificate warnings (Ignorer les avertissements de certificat). Nous vous recommandons d'utiliser cette option avec discrétion et de ne l'utiliser que dans des environnements Intranet de confiance.
2. Cliquez sur le lien **Manage Web Server** (Gérer Web Server) qui se trouve dans le coin supérieur droit de l'écran.
3. Entrez les **User Name, Password** (Nom d'utilisateur, mot de passe) et **Domain Name** (Nom de domaine) (si vous accédez à Server Administrator à partir d'un domaine défini), puis cliquez sur **Submit** (Soumettre).
4. Sélectionnez **Active Directory Login** (Ouverture de session Active Directory) pour vous connecter avec Microsoft Active Directory. Voir Utilisation de l'ouverture de session Active Directory.

5. Cliquez sur **Submit** (Soumettre).

   Pour fermer votre session Server Administrator, cliquez sur **Log Out** (Déconnexion) dans la Barre de navigation globale.

   REMARQUE : Lorsque vous lancez Server Administrator avec soit Mozilla Firefox version 3.0 et 3.5 soit Microsoft Internet Explorer version 7.0 ou 8.0, une page d'avertissement intermédiaire peut apparaître pour indiquer qu'il existe un problème avec le certificat de sécurité. Pour assurer la sécurité du système, il est recommandé de générer un nouveau certificat X.509, réutiliser un certificat X.509 existant, ou importer un certificat root (racine) ou une chaîne de certificat depuis une autorité de certification (CA). Pour éviter la survenue de tels messages d'avertissement concernant le certificat, celui-ci doit provenir d'une autorité de certification de confiance. Pour en savoir plus sur la gestion de certificats X.509, voir Gestion de certificats X.509.

   REMARQUE : Pour assurer la sécurité du système, il est recommandé d'importer un certificat root (racine) ou une chaîne de certificat depuis une autorité de certification (CA). Pour en savoir plus, voir la documentation VMware.

   REMARQUE : Si l'autorité du certificat est valide et si le Server Administrator Web Server rapporte encore une erreur de certificat sans confiance, vous pouvez tout de même rendre l'autorité de certification une CA de confiance à l'aide du fichier **certutil.exe**. Pour en savoir plus sur l'accès à ce fichier .exe, voir la documentation de votre système d'exploitation. Sur les systèmes d'exploitation Windows pris en charge, vous pouvez également utiliser l'option « snap-in » des certificats pour importer les certificats.

Utilisation de l'ouverture de session Active Directory

Vous devez cocher la case **Active Directory Login** (Ouvrir une session Active Directory) pour ouvrir une session à l'aide de la solution de schéma étendu Dell dans Active Directory.

Cette solution vous permet de donner l'accès à Server Administrator, ce qui signifie qu'elle vous permet d'ajouter/contrôler les utilisateurs Server Administrator et les privilèges des utilisateurs existants dans votre logiciel Active Directory. Pour en savoir plus, voir « Using Microsoft Active Directory » (Utilisation de Microsoft Active Directory) dans le *Dell OpenManage Installation and Security User's Guide* (Guide d'utilisation de l'installation et de la sécurité de Dell OpenManage Server Administrator) disponible à l'adresse **dell.com/support/manuals**.

Connexion directe

L'option Single Sign-On (Connexion directe) des systèmes d'exploitation Windows permet à tous les utilisateurs connectés d'accéder directement à l'application Web de Server Administrator en cliquant sur l'icône de **Dell OpenManage Server Administrator** sur le bureau sans passer par la page d'ouverture de session.

REMARQUE : Pour en savoir plus sur la Connexion directe, consultez l'article de la Base de connaissances sur **support.microsoft.com/default.aspx?scid=kb;en-us;Q258063**.

Pour l'accès à l'ordinateur local, vous devez disposer d'un compte sur cet ordinateur et des privilèges appropriés (utilisateur, utilisateur privilégié, ou administrateur). D'autres utilisateurs sont authentifiés avec Microsoft Active Directory. Pour lancer Server Administrator en utilisant l'authentification par connexion directe au lieu de Microsoft Active Directory, vous devez disposer des paramètres suivants :

```
authType=ntlm&application=[plugin name]
```

où `plugin name = omsa, ita,` etc.

Par exemple :

```
https://localhost:1311/?authType=ntlm&application=omsa
```

Pour lancer Server Administrator en utilisant l'authentification par connexion directe au lieu des comptes d'utilisateur sur l'ordinateur local, vous devez disposer des paramètres suivants :

`authType=ntlm&application=[plugin name]&locallogin=true`

où `plugin name = omsa, ita,` etc.

Par exemple :

`https://localhost:1311/?authType=ntlm&application=omsa&locallogin=true`

Server Administrator a également été étendu pour permettre à d'autres produits (comme Dell OpenManage IT Assistant) d'accéder directement aux pages Web de Server Administrator sans passer par la page d'ouverture de session (si vous êtes déjà connecté et si vous disposez des privilèges appropriés).

Configuration des paramètres de sécurité sur des systèmes exécutant un système d'exploitation Microsoft Windows pris en charge

Vous devez configurer les paramètres de sécurité de votre navigateur pour ouvrir une session sur Server Administrator depuis un système de gestion distant qui exécute un système d'exploitation Microsoft Windows pris en charge.

Les paramètres de sécurité de votre navigateur peuvent empêcher aux scripts côté client utilisés par Server Administrator de s'exécuter. Pour autoriser l'utilisation des scripts côté client, réalisez les étapes suivantes sur le système de gestion distant.

REMARQUE : Si vous n'avez pas configuré votre navigateur pour qu'il autorise l'utilisation des scripts côté client, il est possible qu'un écran vide s'affiche lorsque vous ouvrez une session sur Server Administrator. Dans ce cas, un message d'erreur s'affiche et vous indique comment configurer les paramètres de votre navigateur.

Activation de l'utilisation des scripts côté client sur Internet Explorer

1. Dans votre navigateur Web, cliquez sur **Tools** → **Internet Options** → **Security** (Outils > Options Internet > Sécurité).

   La fenêtre **Internet Options** s'affiche.
2. Sous **Select a zone to view or change security settings** (Sélectionner une zone pour afficher ou modifier les paramètres de sécurité), cliquez sur **Trusted Sites** (Sites de confiance), puis sur **Sites**.
3. Dans le champ **Add this website to the zone** (Ajouter ce site Web à la zone), collez l'adresse Web utilisée pour accéder au système géré distant.
4. Cliquez sur **Add** (Ajouter).
5. Copiez l'adresse Web utilisée pour accéder au système géré distant depuis la barre d'adresse du navigateur et collez-la dans le champ **Add this Web Site to the Zone**.
6. Sous **Security level for this zone** (Niveau de sécurité pour cette zone), cliquez sur **Custom Level** (Personnaliser le niveau).

   Pour Windows Server 2003 :

   a. Sous **Miscellaneous** (Divers), sélectionnez **Allow Meta Refresh** (Autoriser l'actualisation des métadonnées).
   b. Sous **Active Scripting** (Scripts actifs), sélectionnez **Enable** (Activer).
   c. Sous **Scripts actifs**, sélectionnez **Allow scripting of Internet Explorer web browser controls** (Autoriser les scripts des commandes de navigation Web d'Internet Explorer).
7. Cliquez sur **OK** pour enregistrer les nouveaux paramètres.
8. Fermez le navigateur et ouvrez une session Server Administrator.

Activation de l'authentification unique pour Server Administrator sur Internet Explorer

Pour autoriser l'authentification unique pour Server Administrator sans être invité à saisir les références utilisateur :

1. Dans votre navigateur Web, cliquez sur **Tools** → **Internet Options** → **Security** (Outils > Options Internet > Sécurité).
2. Sous **Select a zone to view or change security settings** (Sélectionner une zone pour afficher ou modifier les paramètres de sécurité), cliquez sur **Trusted Sites** (Sites de confiance), puis sur **Sites**.
3. Dans le champ **Add this website to the zone** (Ajouter ce site Web à la zone), collez l'adresse Web utilisée pour accéder au système géré distant.

4. Cliquez sur **Ajouter**.
5. Cliquez sur **Custom Level** (Niveau personnalisé).
6. Sous **User Authentication** (Authentification utilisateur), sélectionnez **Automatic Logon with current username and password** (Connexion automatique avec le nom d'utilisateur et mot de passe actuels).
7. Cliquez sur **OK** pour enregistrer les nouveaux paramètres.
8. Fermez le navigateur et ouvrez une session Server Administrator.

Activation de l'utilisation des scripts côté client sur Mozilla Firefox

1. Ouvrez votre navigateur.
2. Cliquez sur **Edit** → **Preferences** (Modifier > Préférences).
3. Sélectionnez **Advanced** → **Scripts and Plugins** (Avancé > Scripts et Plug-ins).
4. Sous Enable Javascript for (Activer Javascript pour), assurez-vous que Navigator (Navigateur) est sélectionné. Assurez-vous que la case **Navigator** est cochée sous **Enable JavaScript for**.
5. Cliquez sur **OK** pour enregistrer les nouveaux paramètres.
6. Fermez le navigateur.
7. Ouvrez une session sur Server Administrator.

Page d'accueil de Server Administrator

REMARQUE : N'utilisez pas les boutons de barre d'outils de votre navigateur Web (**Back** (Précédent) et **Refresh** (Actualiser), notamment) pendant l'utilisation de Server Administrator. Utilisez uniquement les outils de navigation Server Administrator.

À quelques exceptions près, la page d'accueil de Server Administrator présente trois zones principales :

- La barre de navigation globale, qui fournit des liens vers des services généraux.
- L'arborescence système, qui affiche tous les objets système visibles en fonction des privilèges d'accès de l'utilisateur.
- Le fenêtre d'actions, qui affiche les actions de gestion disponibles pour l'objet de l'arborescence système sélectionné en fonction des privilèges d'accès de l'utilisateur. Cette fenêtre contient trois zones fonctionnelles :
  - Les onglets Action, qui affichent les actions principales ou les catégories d'actions disponibles pour l'objet sélectionné en fonction des privilèges d'accès de l'utilisateur.
  - Les onglets d'action sont divisés en sous-catégories comportant toutes les options secondaires disponibles pour les onglets d'action en fonction des privilèges d'accès de l'utilisateur.
  - La zone de données, qui affiche des informations pour l'objet sélectionné dans l'arborescence système, l'onglet Action et le sous-onglet, en fonction des privilèges d'accès de l'utilisateur.

En outre, lorsque la page d'accueil de **Server Administrator** est ouverte, le modèle du système, le nom attribué au système, le nom d'utilisateur de l'utilisateur qui a ouvert la session et les privilèges utilisateur sont affichés dans le coin supérieur droit de la fenêtre.

Lorsque Server Administrator est installé sur le système, le tableau suivant répertorie les noms des champs de l'**interface utilisateur graphique** et le système concerné.

Tableau 6. Noms des champs de l'interface utilisateur graphique et systèmes applicables

Nom de champ de l'interface utilisateur graphique	Système concerné
Enceinte modulaire	Système modulaire
Module serveur	Système modulaire
Système principal	Système modulaire

System	Système non-modulaire
Châssis principal du système	Système non-modulaire

La figure suivante illustre un exemple de page d'accueil de Server Administrator pour un utilisateur ayant ouvert une session avec des privilèges d'administrateur sur un système non modulaire.

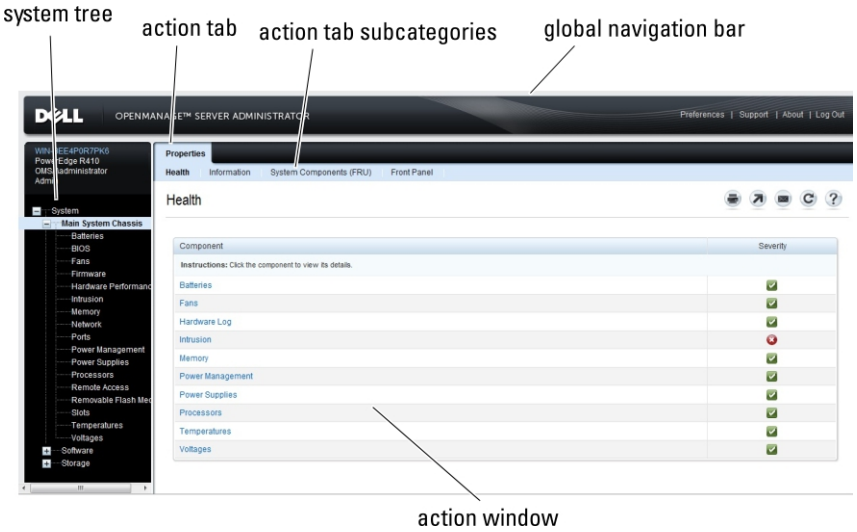

Figure 1. Exemple de page d'accueil de Server Administrator — Système non modulaire

La figure suivante illustre un exemple de page d'accueil de Server Administrator pour un utilisateur ayant ouvert une session avec des privilèges d'administrateur sur un système modulaire.

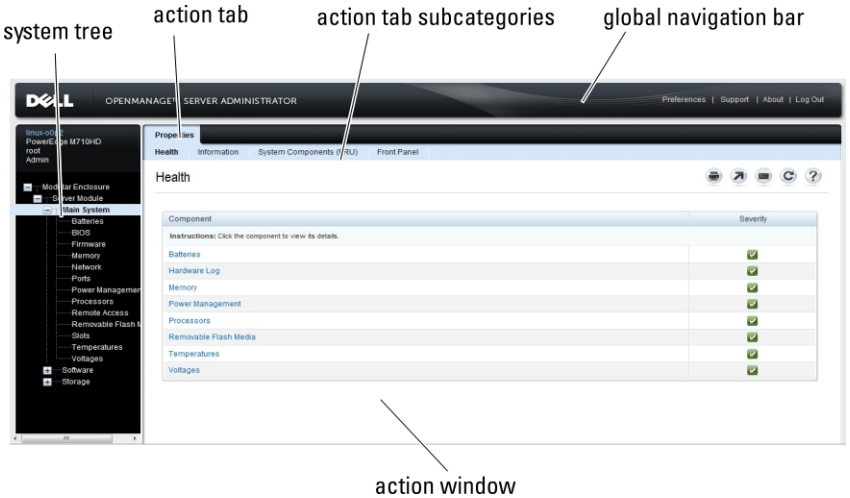

Figure 2. Exemple de page d'accueil de Server Administrator — Système modulaire

Le fait de cliquer sur un objet dans l'arborescence système ouvre une fenêtre d'actions correspondante pour cet objet. Vous pouvez naviguer la fenêtre d'actions en cliquant sur les onglets d'action pour sélectionner les catégories principales et en cliquant sur les sous-catégories des onglets d'action pour accéder à des informations plus détaillées ou des actions plus ciblées. Les informations qui sont affichées dans la zone de données de la fenêtre d'actions peuvent aller de journaux système aux voyants d'état et jauges des capteurs du système. Lorsque des éléments sont soulignés dans la zone de données de la fenêtre d'action, cela signifie qu'ils possèdent un niveau de fonctionnalité plus important. Le fait de cliquer sur un élément souligné entraîne la création d'une nouvelle zone de données dans la fenêtre d'action

qui contient davantage de détails. Par exemple, si vous cliquez sur **Main System Chassis/Main System** (Châssis du système principal/Système principal) dans la sous-catégorie **Health** (Intégrité) de l'onglet d'action **Properties** (Propriétés), cela entraîne la création d'une liste dans laquelle est répertoriée la condition d'intégrité de tous les composants de l'objet Main System Chassis/Main System dont la condition d'intégrité est surveillée.

REMARQUE : Les privilèges d'administrateur ou d'utilisateur privilégié sont requis pour afficher la plupart des objets de l'arborescence système, composants système, onglets d'action et fonctionnalités des zones de données configurables. En outre, seuls les utilisateurs qui se sont connectés avec des privilèges d'administrateur peuvent accéder aux fonctionnalités système critiques telles que la fonctionnalité d'arrêt incluse sous l'onglet **Shutdown** (Arrêt).

Différences d'interface utilisateur de Server Administrator au sein des systèmes modulaires et non modulaires

Le tableau suivant répertorie la disponibilité des fonctionnalités de Server Administrator au sein des systèmes modulaires et non modulaires.

Tableau 7. Différences d'interface utilisateur de Server Administrator au sein des systèmes modulaires et non modulaires

Fonctions	Système modulaire	Système non-modulaire
Batteries	✓	✓
Blocs d'alimentation	✗	✓
Ventilateurs	✗	✓
Performances matérielles	✗	✓ (10G et versions ultérieures)
Intrusion	✗	✓
Mémoire	✓	✓
Network (Réseau)	✓	✓
Ports	✓	✓
Power Management (Gestion de l'alimentation)	✓	✓ (10G et versions ultérieures)
Processeurs	✓	✓
Accès à distance	✓	✓
Média flash amovible	✓	✓
Logements	✓	✓
Températures	✓	✓

Fonctions	Système modulaire	Système non-modulaire
Tensions		
Enceinte modulaire (Informations sur le châssis et sur CMC)		

Barre de navigation globale

La barre de navigation globale et ses liens peuvent être utilisés à tous les niveaux d'utilisateurs dans le programme.

- Cliquez sur **Preferences** (Préférences) pour ouvrir la page d'accueil **Preferences**. Voir Utilisation de la page d'accueil des préférences.
- Cliquez sur **Support** (Prise en charge) pour établir une connexion au site Web de support Dell.
- Cliquez sur **About** (À propos de) pour afficher la version de Server Administrator et les informations de copyright.
- Cliquez sur **Log Out** (Fermer la session) pour mettre fin à la session actuelle du programme Server Administrator.

Arborescence système

L'arborescence système apparaît à gauche sur la page d'accueil de Server Administrator et répertorie les composants affichables de votre systèmes. Les composants système sont classés par type. Lorsque vous développez l'objet principal appelé **Modular Enclosure** → **System/Server Module** (Système de l'enceinte modulaire/Module serveur) les catégories principales de composants du système/module serveur pouvant apparaître sont **Main System Chassis/Main System** (Châssis du système principal/Système principal), **Software** (Logiciel) et **Storage** (Stockage).

Pour développer une branche de l'arborescence, cliquez sur le signe plus () à gauche d'un objet, ou double-cliquez sur l'objet. Un signe moins () indique qu'une entrée développée ne peut pas être développée davantage.

Fenêtre d'action

Lorsque vous cliquez sur un élément dans l'arborescence système, les détails du composant/de l'objet s'affichent dans la zone de données de la fenêtre d'action. Cliquez sur un onglet Action pour afficher toutes les options utilisateur disponibles, sous forme de liste de sous-onglets ou de sous-catégories.

Le fait de cliquer sur un objet de l'arborescence système/module serveur ouvre la fenêtre d'action de ce composant et affiche tous les onglets d'action disponibles. La zone de données revient par défaut à la sous-catégorie présélectionnée du premier onglet d'action pour l'objet sélectionné.

La sous-catégorie présélectionnée correspond généralement à la première option. Par exemple, le fait de cliquer sur l'objet **Main System Chassis/Main System** (Châssis du système principal/Système principal) entraîne l'ouverture d'une fenêtre d'action dans laquelle l'onglet d'action **Properties** (Propriétés) et la sous-catégorie **Health** (Intégrité) sont affichés dans la zone de données de la fenêtre.

Zone de données

La zone de données se trouve en dessous des onglets d'action, à droite sur la page d'accueil. La zone de données sert à réaliser des tâches ou afficher des détails concernant les composants système. Le contenu de la fenêtre dépend de l'objet de l'arborescence système et de l'onglet d'action actuellement sélectionnés. Par exemple, lorsque vous sélectionnez **BIOS** dans l'arborescence système, l'onglet **Properties** (Propriétés) est sélectionné par défaut et les informations de version du BIOS du système apparaissent dans la zone de données. La zone de données de la fenêtre d'action contient un grand nombre de fonctions communes, notamment les voyants d'état, les boutons de tâches, les éléments soulignés, et les indicateurs de niveau.

L'interface utilisateur Server Administrator affiche la date au format <jj/mm/aaaa>.

Indicateurs de condition des composants de système/module de serveur

Les icônes qui apparaissent en regard des noms des composants indiquent la condition de ce composant particulier (telle qu'elle était au dernier rafraîchissement de la page).

Tableau 8. Indicateurs de condition des composants de système/module de serveur

Description	Icône
le composant est intègre (normal).	
Le composant a une condition d'avertissement (non critique). Une condition d'avertissement survient lorsqu'un capteur ou autre outil de surveillance détecte qu'une mesure d'un composant a certaines valeurs minimales et maximales. Une condition d'avertissement nécessite une intervention immédiate.	
Le composant a une condition d'échec ou critique. Une condition critique survient lorsqu'un capteur ou autre outil de surveillance détecte qu'une mesure d'un composant a certaines valeurs minimales et maximales. Une condition critique nécessite une intervention immédiate.	
La condition d'intégrité du composant est inconnue.	

Boutons de tâches

La plupart des fenêtres ouvertes depuis la page d'accueil de Server Administrator contiennent au moins cinq boutons de tâches : **Print** (Imprimer), **Export** (Exporter), **Email**, **Help** (Aide) et **Refresh** (Actualiser). D'autres boutons de tâches sont inclus dans les fenêtres spécifiques de Server Administrator. La fenêtre **Log** (Journal), par exemple, contient également les boutons de tâches **Save As** (Enregistrer sous) et **Clear Log** (Effacer le journal).

- Si vous cliquez sur **Print** ( ), une copie de la fenêtre ouverte s'imprime sur votre imprimante par défaut.
- Si vous cliquez sur **Export** ( ), cela génère un fichier texte qui répertorie les valeurs de chaque champ de données de la fenêtre ouverte. Le fichier d'exportation est enregistré sur un emplacement de votre choix. Pour en savoir plus sur la personnalisation du délimiteur qui sépare les valeurs des champs de données, voir « Setting User » (Configurer l'utilisateur) et « System Preferences » (Préférences système).
- Si vous cliquez sur **Email** ( ), cela crée un message email adressé au destinataire email que vous avez spécifié. Pour des instructions pour configurer le serveur email et le destinataire email par défaut, voir « Setting User » et « System Preferences ».
- Si vous cliquez sur **Refresh** (Actualiser) ( ), les informations sur la condition des composants du système sont rechargées dans la zone des données de la fenêtre d'action.
- Si vous cliquez sur **Save As**, un fichier HTML de la fenêtre d'action est enregistré dans un fichier **.zip**.
- Si vous cliquez sur **Clear Log**, tous les événements du journal affichés dans la zone de données de la fenêtre d'action sont supprimés.
- Si vous cliquez sur **Help** (Aide) (, des informations détaillées concernant la fenêtre spécifique ou le bouton de tâche affiché apparaissent.

REMARQUE : Les boutons **Export** (Exporter), **Email** et **Save As** (Enregistrer sous) sont uniquement visibles par les utilisateurs connectés avec des privilèges d'utilisateur privilégié ou d'administrateur. Le bouton **Clear Log** est visible uniquement pour les utilisateurs dotés de privilèges d'administrateur.

Éléments soulignés

Si vous cliquez sur un élément souligné dans la zone de données de la fenêtre d'action, des détails supplémentaires sur cet élément s'affichent.

Indicateurs de niveau

Les capteurs de température, des ventilateurs et de tension sont tous représentés par un indicateur de niveau. Par exemple, la figure suivante illustre les résultats d'un capteur de ventilateur de l'UC.

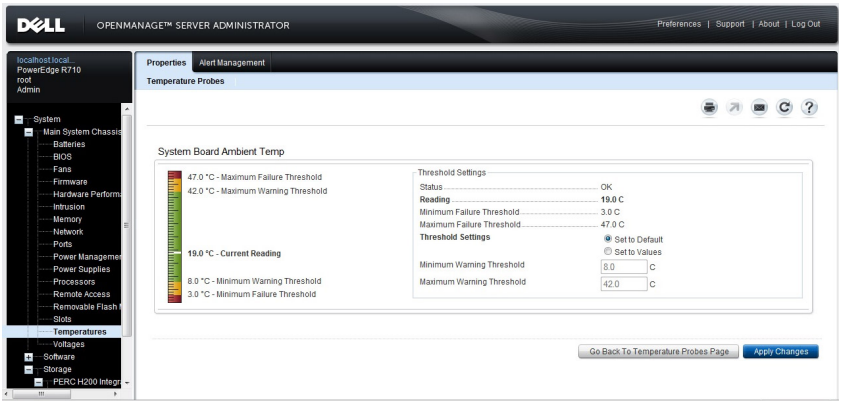

Figure 3. Indicateur de niveau

Utilisation de l'aide en ligne

Une aide en ligne sensible au contexte est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. Cliquez sur **Help** (Aide) pour ouvrir une fenêtre d'aide indépendante qui renferme des informations détaillées concernant la fenêtre spécifique que vous êtes en train de consulter. L'aide en ligne est conçue pour vous guider tout au long des actions spécifiques requises afin de tirer profit de tous les aspects des services de Server Administrator. L'aide en ligne est disponible pour toutes les fenêtres que vous pouvez consulter, en fonction des groupes matériels et logiciels que Server Administrator découvre sur votre système et de votre niveau de privilège d'utilisateur.

Utilisation de la page d'accueil Préférences

Le panneau gauche de la page d'accueil Préférences (là où s'affiche l'arborescence du système sur la page d'accueil de Server Administrator) affiche toutes les options de configuration disponibles dans la fenêtre de l'arborescence du système.

Les options de configuration disponibles de la page d'accueil Préférences sont les suivantes :

- Paramètres généraux
- Server Administrator

Vous pouvez afficher l'onglet **Preferences** (Préférences) une fois que vous êtes connecté pour gérer un système distant. Cet onglet est également disponible lorsque vous vous connectez pour gérer Server Administrator Web Server ou le système local.

Tout comme la page d'accueil de Server Administrator, la page d'accueil **Preferences** présente trois zones principales :

- La barre de navigation globale, qui fournit des liens vers des services généraux.
  - Cliquez sur **Home** (Accueil) pour revenir à la page d'accueil de Server Administrator.

- Le panneau gauche de la page d'accueil **Preferences** (là où s'affiche l'arborescence du système sur la page d'accueil de Server Administrator) affiche les différentes catégories de préférences du système géré ou Server Administrator Web Server.
- La fenêtre d'action affiche les paramètres disponibles et les préférences du système géré ou de Server Administrator Web Server.

La figure suivante présente un exemple de la disposition de la page d'accueil Preferences (Préférences).

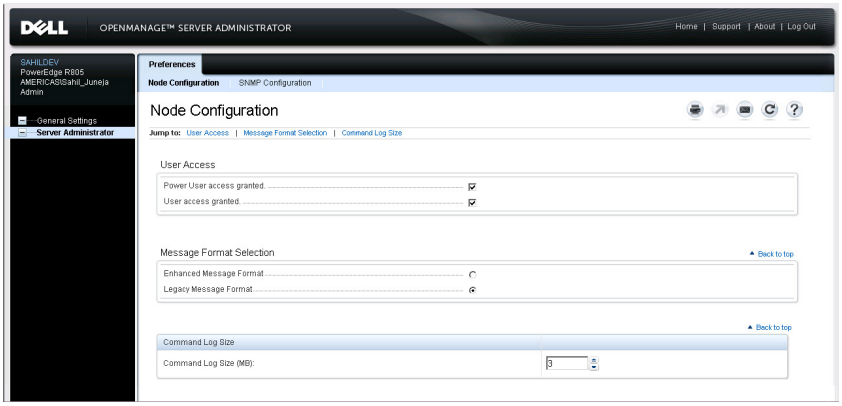

Figure 4. Exemple de page d'accueil Preferences - Managed System (Préférences - Système géré)

Préférences du système géré

Lorsque vous ouvrez une session sur un système distant, la page d'accueil Preferences (Préférences) revient par défaut à la fenêtre Node Configuration (Configuration des nœuds) sous l'onglet **Preferences**.

Cliquez sur l'objet Server Administrator pour autoriser ou interdire l'accès aux utilisateurs dotés de privilèges d'utilisateur ou d'utilisateur privilégié. Selon les privilèges du groupe de l'utilisateur, la fenêtre d'actions de l'objet Server Administrator peut comporter l'onglet **Preferences** ou non.

Sous l'onglet Preferences, vous pouvez :

- Autoriser ou interdire l'accès aux utilisateurs dotés de privilèges d'utilisateur ou d'utilisateur privilégié
- Sélectionner le format des messages d'alerte

  REMARQUE : Les formats possibles sont les suivants : **traditional** (traditionnel) et **enhanced** (optimisé). Le format par défaut est **traditional**, le format hérité.
- Configurer la taille du journal des commandes
- Configurer le protocole SNMP

Préférences de Server Administrator Web Server

Lorsque vous ouvrez une session pour gérer Server Administrator Web Server, la page d'accueil **Preferences** (Préférences) revient par défaut à la fenêtre User Preferences (Préférences utilisateur) sous l'onglet Preferences.

En raison de la séparation de Server Administrator Web Server du système géré, les options suivantes s'affichent lorsque vous ouvrez une session Server Administrator Web Server, via le lien Manage Web Server (Gérer Web Server) :

- Préférences de Web Server
- Gestion du certificat X.509

Pour en savoir plus sur comment accéder à ces fonctions, consultez le document Présentation des services de Server Administrator.

Service de connexion Dell Systems Management Server Administration et configuration de la sécurité

Configuration des préférences utilisateur et système

La page d'accueil **Preferences** (Préférences) permet de définir les préférences utilisateur et système de port sécurisé.

REMARQUE : Vous devez être connecté avec des privilèges d'administrateur pour définir ou redéfinir des préférences utilisateur ou système.

Pour définir vos préférences utilisateur :

1. Cliquez sur **Preferences** sur la barre de navigation globale.

   La page d'accueil Preferences apparaît.
2. Cliquez sur **General Settings** (Paramètres généraux).
3. Pour ajouter un destinataire d'e-mail présélectionné, tapez l'adresse e-mail de votre contact désigné pour le service dans le champ **Mail To** (Destinataire), puis cliquez sur **Apply** (Appliquer).

   REMARQUE : Si vous cliquez sur E-mail () dans une fenêtre, un e-mail est envoyé avec, en pièce jointe, un fichier HTML de la fenêtre à l'adresse e-mail désignée.

   REMARQUE : L'URL de Web Server n'est pas conservée si vous redémarrez le service OpenManage Server Administrator ou le système sur lequel Server Administrator est installé. Utilisez la commande omconfig pour saisir à nouveau l'URL.

Système de port sécurisé

Effectuez les étapes suivantes pour configurer vos préférences système de port sécurisé :

1. Cliquez sur **Préférences** sur la barre de navigation globale.

   La page d'accueil **Preferences** (Préférences) apparaît.
2. Cliquez sur **Paramètres généraux**.
3. Dans la fenêtre **Server Preferences** (Préférences serveur), définissez les options souhaitées.

   - La fonction **Session Timeout (minutes)** (Délai d'attente de la session (minutes)) peut être utilisée pour définir une limite au temps pendant lequel une session Server Administrator peut rester active. Sélectionnez **Enable** (Activer) pour autoriser Server Administrator à expirer si aucune interaction utilisateur ne survient pendant une durée spécifiée (en minutes). Les utilisateurs dont la session expire doivent se reconnecter pour continuer. Sélectionnez **Disable** (Désactiver) si vous souhaitez désactiver la fonction **Session Timeout (minutes)** de Server Administrator.
   - Le champ **HTTPS Port** (port HTTPS) spécifie le port sécurisé pour Server Administrator. Le port sécurisé par défaut pour Server Administrator est 1311.

     REMARQUE : Si vous modifiez le port et le définissez sur un numéro de port non valide ou utilisé, cela peut empêcher d'autres applications ou navigateurs d'accéder à Server Administrator sur le système géré. Pour obtenir une liste des ports par défaut, voir le *Dell OpenManage Installation and Security User's Guide* (Guide d'installation et de sécurité de Dell OpenManage).
   - Le champ **IP Address to Bind** (Adresse IP à lier) spécifie la ou les adresses IP du système géré auxquelles Server Administrator se lie au démarrage d'une session. Sélectionnez **All** (Toutes) pour lier toutes les adresses IP applicables de votre système. Sélectionnez **Specific** (Spécifique) pour lier une adresse IP spécifique.

     REMARQUE : Si vous donnez une autre valeur que **All** au champ **IP Address to Bind**, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré.
   - Le champ **Mail To** (Envoyer à) spécifie la ou les adresses auxquelles vous souhaitez envoyer des emails concernant les mises à jour par défaut. Vous pouvez configurer plusieurs adresses emails en les séparant pas une virgule.

- Les champs **SMTP Server Name (or IP Address)** (Nom du serveur SMTP (ou adresse IP) et **DNS Suffix for SMTP Server** (Suffixe DNS du serveur SMTP) spécifient le protocole SMTP et le suffixe DNS (serveur de nom de domaine) de votre entreprise ou organisation. Pour permettre à Server Administrator d'envoyer des emails, vous devez saisir les adresses IP et le suffixe DNS du serveur SMTP de votre entreprise ou organisation dans les champs appropriés.

  REMARQUE : Pour des raisons de sécurité, votre entreprise ou organisation peut interdire l'envoi d'e-mails à des comptes extérieurs via le serveur SMTP.

- Le champ **Command Log Size** (Taille du journal des commandes) spécifie la taille de fichier maximale en Mo du fichier du journal des commandes.

  REMARQUE : Ce champ apparaît uniquement lorsque vous ouvrez une session pour gérer Server Administrator Web Server.

- Le champ **Support Link** (Lien d'assistance) précise l'URL de la société qui fournit un support pour votre système géré.
- Le champ **Custom Delimiter** (Délimiteur personnalisé) spécifie le caractère utilisé pour séparer les champs de données dans les fichiers créés à l'aide du bouton **Exporter**. Le caractère **;** est le délimiteur par défaut. Les autres options disponibles sont **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **|** et **,**.
- Le champ **SSL Encryption** (Cryptage SSL) spécifie les niveaux de cryptage des sessions HTTPS sécurisées. Les niveaux de cryptage disponibles incluent : **Auto Negotiate** (Négociation automatique) et **128-bit or Higher** (128 bits ou plus).

  – **Auto Negotiate** (Négociation automatique) : permet de se connecter depuis un navigateur, peut importe son niveau de cryptage. Le navigateur négocie automatiquement avec Server Administrator Web Server et utilise le plus haut niveau de cryptage disponible pour la session. Les navigateurs hérités à cryptage plus faible peuvent également se connecter à Server Administrator.

  – **128-bit or Higher** (128 bits ou plus) : permet de se connecter depuis des navigateurs disposant d'un niveau de cryptage de 128 bits ou plus. Une des suites de cryptage suivantes est applicable, en fonction du navigateur d'une des sessions établies :

```
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

  REMARQUE : L'option **128-bit or Higher** ne vous permet pas de vous connecter à partir d'un navigateur avec un niveau de cryptage SSL inférieur, tel que 40 bits et 56 bits.

- **Key Signing Algorithm (For Self Signed Certificate)** (Algorithme de signature clé (pour le certificat auto-signé)) : vous permet de sélectionner un algorithme de signature pris en charge. Si vous sélectionnez l'algorithme **SHA 512** ou **SHA 256**, assurez-vous que votre système d'exploitation/navigateur le prend en charge. Si vous sélectionnez l'une de ces options sans la prise en charge du système d'exploitation/navigateur nécessaire, Server Administrator affiche l'erreur suivante : `cannot display the webpage` (Impossible d'afficher la page Web). Ce champ est destiné uniquement aux certificats auto-signés et auto-générés de Server Administrator. La liste déroulante est grisée si vous importez ou générer de nouveaux certificats dans Server Administrator.

- **Java Runtime Environment** (Environnement d'exécution Java) : vous permet de sélectionner l'une des options suivantes :
- **Bundled JRE** (Environnement d'exécution Java groupé) : permet d'utiliser le JRE fourni avec le System Administrator.
- **System JRE** (Système d'environnement d'exécution Java) : permet d'utiliser le JRE installé sur le système. Sélectionnez la version requise dans la liste déroulante.

REMARQUE : Si le JRE n'existe pas sur le système sur lequel Server Administrator s'exécute, le JRE fourni avec Server Administrator est utilisé.

REMARQUE : Si le niveau de cryptage est défini sur **128-bit or Higher**, vous pouvez accéder aux paramètres de Server Administrator ou les modifier avec un navigateur ayant les mêmes niveaux de cryptage ou des niveaux plus élevés.

4. Une fois que vous avez terminé de définir les options dans la fenêtre **Server Preferences** (Préférences serveur), cliquez sur **Apply** (Appliquer les changements).

   REMARQUE : Vous devez redémarrer Server Administrator Web Server pour que les changements deviennent effectifs.

Gestion du certificat X.509

REMARQUE : Vous devez avoir ouvert une session avec des privilèges d'administrateur pour pouvoir effectuer la gestion des certificats.

Des certificats Web sont nécessaires pour vérifier l'identité d'un système distant et pour s'assurer que les informations échangées avec le système distant ne puissent pas être lues ou modifiées par d'autres utilisateurs. Pour assurer la sécurité du système, nous vous recommandons de :

- Générer un nouveau certificat X.509, réutiliser un certificat X.509 existant ou importer un certificat racine ou une chaîne de certificats d'une autorité de certification (AC).
- Tous les systèmes sur lesquels Server Administrator est installé doivent avoir des noms d'hôte uniques.

Pour gérer des certificats X.509 via la page d'accueil **Preferences** (Préférences), cliquez sur **General Settings** (Paramètres généraux), cliquez sur l'onglet **Web Server**, puis sur **X.509 Certificate** (Certificat X.509).

Les options disponibles sont les suivantes :

- **Generate a new certificate** (Générer un nouveau certificat) : génère un nouveau certificat auto-signé utilisé pour la communication SSL entre le serveur fonctionnant sous Server Administrator et le navigateur.

  REMARQUE : Lors de l'utilisation d'un certificat auto-signé, la plupart des navigateurs Web affichent un avertissement *untrusted* (non sécurisé) car le certificat auto-signé n'est pas signé par une autorité de certification (AC) de confiance du système d'exploitation. Certains paramètres de navigateur sécurisés peuvent également bloquer les certificats SSL auto-signés. L'interface GUI Web OMSA requiert un certificat signé par une autorité de certification pour de tels navigateurs sécurisés.
- **Certificate Maintenance** (Maintenance de certificats) : vous permet de générer une requête de signature de certificat (RSC) comprenant des informations sur l'hôte requis par l'autorité de certification pour automatiser la création d'un certificat Web SSL de confiance. Vous pouvez récupérer le fichier RSC nécessaire depuis les instructions qui figurent sur la page (RSC) ou en copiant le texte complet dans la boîte de texte qui se trouvent sur la page de RSC et en le collant dans le formulaire de l'autorité de certification. Le texte doit être au format codé Base64.

  REMARQUE : Vous pouvez également afficher les informations du certificat et exporter le certificat en cours d'utilisation au format Base–64 universel, qui peut être importé par d'autres services Web.
- **Import a root certificate** (Importer un certificat racine) : généralement, une autorité de certification émet un fichier de certificat racine (selon le nom de domaine de l'hôte) et un fichier de chaîne de certificat qui établit la confiance entre l'autorité de certificat, le certificat racine de l'hôte et le navigateur web et le système d'exploitation d'un utilisateur distant. Pour des domaines plus larges, le fichier de chaîne de certificat définit les autorités de certification intermédiaires. En premier lieu, importez le fichier de certificat racine (généralement un fichier de type .CER) de l'hôte. Ensuite, importez la chaîne de certificats PKCS#7 émise par une autorité de certification (généralement un fichier de type .P7B) et qui établit la chaîne de confiance depuis l'autorité de certification de premier niveau via des autorités intermédiaires approuvées par le système d'exploitation vers le certificat racine.
- **Import certificate chain** (Importer une chaîne de certificats) : vous permet d'importer la réponse du certificat (au format PKCS#7) reçue d'une autorité de certification de confiance.

Onglets d'actions de Server Administrator Web Server

Les onglets d'action suivants s'affichent lorsque vous ouvrez une session pour gérer le Server Administrator Web Server :

- Propriétés
- Arrêt
- Journaux
- Gestion des alertes
- Gestion des sessions

Utilisation de l'interface de ligne de commande de Server Administrator

L'interface de ligne de commande (CLI) de Server Administrator permet aux utilisateurs d'effectuer les tâches de gestion de systèmes essentielles via l'invite de commande du système d'exploitation d'un système surveillé.

La CLI permet à un utilisateur qui sait exactement ce qu'il veut d'obtenir rapidement des informations sur le système. Les commandes CLI, par exemple, permettent aux administrateurs d'écrire des programmes séquentiels ou des scripts pour qu'ils s'exécutent à un moment particulier. Lorsque ces programmes s'exécutent, ils peuvent capturer des rapports sur des composants intéressants, tels que les RPM (tours par minute) des ventilateurs. Grâce aux scripts supplémentaires, la CLI peut être utilisée pour capturer des données pendant des périodes de forte utilisation du système pour les comparer aux données correspondantes capturées pendant des périodes de faible utilisation du système. Les résultats de cette commande peuvent être acheminés vers un fichier pour une analyse ultérieure. Les rapports peuvent aider les administrateurs à obtenir des informations pouvant être utilisées pour régler les tendances d'utilisation, justifier l'achat de nouvelles ressources système, ou s'intéresser à l'intégrité d'un composant défaillant.

Pour des instructions complètes sur la fonctionnalité et l'utilisation de la CLI, consultez le *Dell OpenManage Server Administrator Command Line Interface Guide* (Guide d'utilisation de l'interface de ligne de commande de Dell OpenManage Server Administrator) à l'adresse **dell.com/support/manuals**.

4

Services Server Administrator

Le Dell OpenManage Server Administrator Instrumentation Service surveille l'intégrité d'un système et fournit un accès rapide aux informations détaillées concernant les défaillances et les performances recueillies par des agents de gestion de systèmes conformes aux normes de l'industrie. Les fonctions de création de rapports et d'affichage permettent d'obtenir la condition d'intégrité générale de chaque châssis compris dans votre système. Au niveau du sous-système, vous pouvez consulter les informations concernant les tensions, températures, tours par minute des ventilateur et fonction de la mémoire à des points clés du système. Vous pouvez consulter un compte-rendu détaillé des coûts de propriété pertinents associés à votre système dans la vue Summary (Résumé). Il est également possible d'obtenir des informations sur la version du BIOS, du micrologiciel, du système d'exploitation et de tous les logiciels de gestion des systèmes installés.

Les administrateurs du système peuvent également utiliser Instrumentation Service pour effectuer les tâches essentielles suivantes :

- Spécifier les valeurs minimum et maximum pour certains composants critiques. Les valeurs, appelées seuils, déterminent la plage dans laquelle un événement d'avertissement survient (les valeurs d'échec minimum et maximum sont spécifiées par le fabricant du système).
- Spécifier la réponse du système lorsqu'un événement d'avertissement ou d'échec survient. Les utilisateurs peuvent configurer les actions qu'un système prend en réponse à des notifications d'événements d'avertissement ou d'échec. En variante, les utilisateurs disposant d'une surveillance 24 h sur 24 peuvent spécifier de ne prendre aucune mesure et se fier au jugement humain pour sélectionner la meilleure action à prendre en réponse à un événement.
- Remplir toutes les valeurs définissables par l'utilisateur pour le système, par exemple, le nom du système, le numéro de téléphone de l'utilisateur principal du système, la méthode d'amortissement, si le système est loué ou acheté, et ainsi de suite.

REMARQUE : Vous devez configurer le service SNMP (Simple Network Management Protocol) pour qu'il accepte les paquets SNMP pour les systèmes gérés et les systèmes de gestion de réseau exécutant Microsoft Windows Server 2003. Pour en savoir plus sur la configuration SNMP, voir Configuration de l'agent SNMP pour les systèmes exécutant des systèmes d'exploitation Windows pris en charge.

Gestion de votre système

La page d'accueil de Server Administrator revient par défaut à l'objet System (Système) de la vue de l'arborescence système. Par défaut, l'objet **System** ouvre les composants **Health** (Intégrité) sous l'onglet **Properties** (Propriétés).

Par défaut, la page d'accueil **Preferences** (Préférences) ouvre **Node Configuration** (Configuration des nœuds).

Dans la page d'accueil **Preferences**, vous pouvez restreindre l'accès aux utilisateurs ayant des privilèges d'utilisateurs ou d'utilisateurs privilégiés, définir le mot de passe SNMP et configurer les paramètres utilisateur et les paramètres du service de connexion SM SA.

REMARQUE : Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. Cliquez sur **Help** (Aide) () pour ouvrir une fenêtre d'aide indépendante contenant des informations détaillées sur la fenêtre spécifique que vous êtes en train de consulter. L'aide en ligne est conçue pour vous guider tout au long des actions spécifiques requises pour explorer tous les aspects des services de Server Administrator. L'aide en ligne est disponible pour toutes les fenêtres que vous pouvez consulter, en fonction des groupes logiciels et matériels que Server Administrator découvre sur votre système et de votre niveau de privilège utilisateur.

REMARQUE : Les privilèges d'administrateur ou d'utilisateur privilégié sont requis pour afficher la plupart des objets de l'arborescence système, composants système, onglets d'action et fonctions de zone de données qui sont configurables. En outre, seuls les utilisateurs connectés avec des privilèges d'administrateur peuvent accéder aux fonctions système critiques, telles que la fonction d'arrêt incluse sous l'onglet **Shutdown** (Arrêt).

Gestion des objets de l'arborescence du système/module de serveur

L'arborescence du système/module de serveur de Server Administrator affiche tous les objets visibles selon les groupes de logiciel et de matériel que Server Administrator découvre sur le système géré et sur les privilèges d'accès de l'utilisateur. Les composants système sont classés par type. Lorsque vous développez l'objet principal — **Modular Enclosure** — **System/Server Module** (Enceinte modulaire > Système/Module de serveur) — les catégories principales des composants système pouvant apparaître sont : **Main System Chassis/Main System** (Châssis de système principal/ Système principal), **Software** (Logiciel) et **Storage** (Stockage).

Si Storage Management Service est installé, selon le contrôleur et le périphérique de stockage relié au système, l'objet de l'arborescence Storage (Stockage) se développe pour afficher divers objets.

Pour des informations détaillées sur le composant Storage Management Service, voir le *Dell OpenManage Server Administrator Storage Management User's Guide* (Guide d'utilisation de Dell OpenManage Server Administrator Storage Management) sur le site **dell.com/support/manuals**.

Objets de l'arborescence du système de la page d'accueil de Server Administrator

Cette section fournit des informations sur les objets de l'arborescence système de la page d'accueil de Server Administrator. En raison des limitations des systèmes d'exploitation VMware ESX et ESXi version 4.X et 5.X, certaines fonctionnalités disponibles dans des versions antérieures d'OpenManage Server Administrator ne sont pas disponibles dans cette version. Ces dernières incluent :

- Informations sur les capacités Fibre Channel sur Ethernet (FCoE) et iSCSI sur Ethernet (iSoE)
- Informations sur les capacités FCoE et iSoE
- Gestion des alertes : Actions d'alerte
- Interface réseau : Condition d'administration, DMA, adresse IP (Internet Protocol - Protocole Internet),
- Interface réseau : Condition d'exploitation
- Préférences : Configuration SNMP
- Arrêt distant : Système de cycle d'alimentation avec arrêt du SE en premier
- À propos des détails : Les détails du composant Server Administrator ne sont pas répertoriés sous l'onglet **Details** (Détails)
- Adressage de rôle

REMARQUE : Server Administrator affiche toujours la date au format <jj/mm/aaaa>.

REMARQUE : Les privilèges d'administrateur ou d'utilisateur privilégié sont requis pour afficher la plupart des objets de l'arborescence système, composants système, onglets d'action et fonctions de zone de données qui sont configurables. En outre, seuls les utilisateurs connectés avec des privilèges d'administrateur peuvent accéder aux fonctions système critiques, telles que la fonction d'arrêt inclue sous l'onglet **Shutdown** (Arrêt).

Enceinte modulaire

REMARQUE : Pour Server Administrator, « enceinte modulaire » fait référence à un système qui peut contenir un ou plusieurs systèmes modulaires apparaissant comme module de serveur distinct dans l'arborescence du système. À l'instar d'un module de serveur, une enceinte modulaire contient tous les composants essentiels d'un système. La seule différence réside dans le fait qu'il existe des logements pour au moins deux modules de serveur dans un conteneur plus grand et que chacun d'entre eux représente un système complet comme module de serveur.

Pour afficher les informations sur le châssis du système modulaire et les informations sur Chassis Management Controller (CMC), cliquez sur l'objet **Modular Enclosure** (Enceinte modulaire).

- **Onglet : Properties (Propriétés)**
- **Sous-onglet : Informations**

Sous l'onglet Properties (Propriétés), vous pouvez :

- Afficher les informations sur le châssis du système modulaire surveillé.
- Afficher des informations détaillées sur Chassis Management Controller (CMC) pour le système modulaire surveillé.

Accès et utilisation de Chassis Management Controller

Pour lancer la fenêtre d'**ouverture de session** du contrôlleur BMC depuis la page d'accueil de Server Administrator :

1. Cliquez sur l'objet **Modular Enclosure** (Enceinte modulaire).
2. Cliquez sur l'onglet **CMC Information** (Informations sur le CMC), puis cliquez sur **Launch the CMC Web Interface** (Lancer l'interface Web CMC). La fenêtre **Log in** (Ouverture de session) CMC apparaît.

Vous pouvez surveiller et gérer votre enceinte modulaire une fois que vous êtes connecté à CMC.

Propriétés du système/Module de serveur

L'objet **System/Server Module** (système/module de serveur) contient trois groupes de composants système principaux : Main System Chassis/Main System (Châssis de système principal), Software (Logiciel) et Storage (Stockage). La page d'accueil de Server Administrator revient par défaut à l'objet **System** (Système) de la vue de l'arborescence système. La plupart des fonctions d'administration sont gérables depuis la fenêtre d'action de l'objet **System/Server Module** (Système/Module de serveur). La fenêtre d'action de l'objet **System/Server Module** comporte les onglets suivants, en fonction des privilèges du groupe de l'utilisateur : **Licensing** (Licences), **Properties** (Propriétés), **Shutdown** (Arrêt), **Logs** (Journaux), **Alert Management** (Gestion des alertes) et **Session Management** (Gestion des sessions).

Licences

Sous-onglets : Information | Licensing (Informations | Licences)

Sous le sous-onglet Licensing, vous pouvez :

- Définir les préférences pour utiliser l'iDRAC (Dell Remote Access Controller) pour importer, exporter, supprimer ou remplacer la licence numérique du matériel.

- Afficher les détails du périphérique utilisé. Les détails incluent la condition de la licence, la description de la licence, l'ID de droit et la date d'expiration de la licence.

  REMARQUE : Server Administrator prend en charge la fonction Licensing (Licences) sur les systèmes PowerEdge12G et versions ultérieures. Cette fonction est disponible uniquement si la version minimale requise de l'iDRAC, iDRAC 1.30.30, est installée.

Propriétés

Sous-onglets : Health | Summary | Asset Information | Auto Recovery (Intégrité | Résumé | Informations sur l'inventaire | Récupération automatique)

Sous l'onglet **Properties** (Propriétés), vous pouvez :

- Afficher la condition actuelle des alertes d'intégrité pour les composants matériels et logiciels de l'objet **Main System Chassis/Main System** (Châssis de système principal/Système principal) et de l'objet **Storage** (Stockage).
- Afficher les informations détaillées du résumé pour tous les composants du système surveillé.
- Afficher et configurer les informations d'inventaire du système surveillé.
- Afficher et définir les actions de récupération automatique du système (registre d'horloge de la surveillance du système d'exploitation) pour le système surveillé.

  REMARQUE : Les options de récupération automatique peuvent ne pas être disponibles si le registre d'horloge de la surveillance du système d'exploitation est activé dans le BIOS. Pour pouvoir configurer les options de récupération automatique, le registre d'horloge de la surveillance doit être désactivé.

  REMARQUE : Les actions de récupération automatique du système peuvent ne pas s'exécuter exactement par période de délai d'attente (n secondes) lorsque l'horloge identifie un système qui ne répond plus. Le temps d'exécution de l'action va de n-h+1 à n+1 secondes, où n correspond à la période de délai d'attente et h correspond à l'intervalle de pulsation. La valeur de l'intervalle de pulsation est 7 secondes lorsque $n \leq 30$ et 15 secondes lorsque $n > 30$.

  REMARQUE : La fonctionnalité de la fonction du registre d'horloge ne peut être garantie lorsqu'un événement de mémoire non corrigible survient dans la mémoire DRAM Bank_1 du système. Si un événement de mémoire non corrigible survient dans cet emplacement, le code BIOS résidant dans cet espace peut devenir corrompu. Étant donné que la fonction d'horloge appelle le BIOS pour effectuer un comportement d'arrêt ou de redémarrage, elle peut ne pas fonctionner correctement. Si cela survient, vous devez redémarrer le système manuellement. Le registre d'horloge peut être défini sur un maximum de 720 secondes.

Arrêt

Sous-onglets : Remote Shutdown | Thermal Shutdown | Web Server Shutdown (Arrêt distant | Arrêt thermique | Arrêt du serveur Web)

Sous l'onglet **Shutdown**, vous pouvez :

- Configurer l'arrêt du système d'exploitation et les options de l'arrêt distant.
- Définir le niveau de gravité de l'arrêt thermique pour arrêter le système si un capteur de température renvoie une valeur d'avertissement ou de panne.

  REMARQUE : Un arrêt thermique survient uniquement lorsque la température rapportée par le capteur dépasse le seuil de température. Aucun arrêt thermique ne survient si la température rapportée par le capteur passe en dessous du seuil de température.
- Arrêter le service de connexion DSM SA (serveur Web).

  REMARQUE : Server Administrator est encore disponible via l'interface de ligne de commande (CLI) lorsque le service de connexion DSM SA est arrêté. Les fonctions CLI ne nécessitent pas que ce service s'exécute.

Journaux

Sous-onglets : Hardware | Alert | Command (Matériel | Alerte | Commande)

Sous l'onglet **Logs** (Journaux), vous pouvez :

- Afficher le journal ESM (Embedded System Management - Journal de gestion du système intégré) ou le journal SEL (System Event Log - Journal d'événements du système) pour voir une liste de tous les événements associés aux

composants du matériel de votre système. L'icône du voyant d'état en regard du nom du journal passe d'une condition normale ( ) à une condition non critique ( ) lorsque le fichier journal atteint une capacité de 80 pour cent. Sur les systèmes Dell PowerEdge 9G et 11G, l'icône du voyant d'état en regard du nom du journal passe à une condition critique ( ) lorsque le fichier journal atteint une capacité de 100 pourcent.

REMARQUE : Nous vous recommandons de vider le journal du matériel lorsqu'il atteint une capacité de 80 pourcent. Si le journal venait à atteindre une capacité de 100 pourcent, les derniers événements seraient supprimés du journal.

- Voir le journal des alertes pour afficher une liste de tous les événements générés par Server Administrator Instrumentation Service quand la condition des capteurs et des autres paramètres surveillés change.

  REMARQUE : Pour en savoir plus sur chaque ID d'événement d'alerte et sur la description de chacun, son niveau de gravité et sa cause, voir le *Server Administrator Messages Reference Guide* (Guide de référence des messages de Server Administrator) à l'adresse **dell.com/support/manuals**.

- Voir le journal des commandes pour afficher une liste de chaque commande exécutée à partir de la page d'accueil de **Server Administrator** ou à partir de son interface de ligne de commande.

  REMARQUE : Pour des instructions sur l'affichage, l'impression, l'enregistrement et l'envoi par e-mail des journaux, voir la section « Journaux de Server Administrator ».

Gestion des alertes

Sous-onglets : Alert Actions | Platform Events | SNMP Traps (Actions d'alerte | Événements sur plateforme| Interruptions SNMP)

Sous l'onglet **Alert Management** (Gestion des alertes), vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si le capteur d'un composant du système donne une valeur d'avertissement ou de panne.
- Afficher les paramètres actuels du Platform Event Filter (Filtre d'événements de plate-forme) et définir les actions de filtrage des événements de plate-forme à réaliser si un capteur de composant système venait à renvoyer une valeur d'avertissement ou de panne. Vous pouvez également utiliser l'option **Configure Destination** (Configurer la destination) pour sélectionner une destination (adresse IPv4 ou IPv6) vers laquelle envoyer une alerte pour un événement de plate-forme.

  REMARQUE : Server Administrator n'affiche pas la référence d'étendue de l'adresse IPv6 dans son interface utilisateur graphique.

- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux des seuils d'alerte pour les composants système instrumentés. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

  REMARQUE : Les actions d'alerte pour tous les capteurs de composants système potentiels sont répertoriées dans la fenêtre **Alert Actions** (Actions d'alerte), même s'ils ne sont pas présents sur le système. La définition d'actions d'alerte pour les capteurs de composants système qui ne se trouvent pas sur votre système n'a aucun effet.

  REMARQUE : Sur tout système d'exploitation Microsoft Windows, l'option **Advanced System Settings → Advanced Recovery** (Paramètres de système avancés > Restauration avancée) du système d'exploitation doit être désactivée pour assurer la génération des alertes Server Administrator Automatic System Recovery (Restauration système automatique de Server Administrator).

Gestion des sessions

Sous-onglets : Session

Sous l'onglet **Session Management** (Gestion des sessions), vous pouvez :

- Afficher les informations sur les sessions des utilisateurs déjà connectés à Server Administrator.
- Mettre fin à des sessions utilisateur.

REMARQUE : Seuls les utilisateurs disposant de privilèges d'administration peuvent afficher la page **Session Management** et mettre fin aux sessions des utilisateurs connectés.

Châssis de système principal/Système principal

Cliquez sur l'objet **Main System Chassis/Main System** (Châssis de système principal/Système principal) pour gérer les composants matériels et logiciels principaux de votre système.

Les composants disponibles sont :

- Batteries
- BIOS
- Ventilateurs
- Micrologiciel
- Performances matérielles
- Intrusion
- Mémoire
- Network (Réseau)
- Ports
- Power Management (Gestion de l'alimentation)
- Blocs d'alimentation
- Processeurs
- Accès à distance
- Média flash amovible
- Logements
- Températures
- Tensions

REMARQUE : Les performances matérielles sont prises en charge uniquement sur les systèmes Dell PowerEdge 10G et versions ultérieures. L'option **Power Supplies** (Blocs d'alimentation) n'est pas disponible sur les systèmes Dell PowerEdge 1900. La gestion de l'alimentation est prise en charge sur certains systèmes Dell PowerEdge 10G et versions ultérieures. Les fonctions Power Supply Monitoring (Surveillance des blocs d'alimentation) et Power Monitoring (Surveillance de l'alimentation) sont disponibles uniquement sur les systèmes sur lesquels sont installés au moins deux blocs d'alimentation redondants remplaçables à chaud. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondants installés définitivement qui ne disposent pas de circuits de gestion de l'alimentation.

Propriétés du châssis de système principal/système principal

Le système/module du serveur peut contenir un châssis de système principal ou plusieurs châssis. Le châssis de système principal/système principal contient les composants essentiels d'un système. Le fenêtre d'action de l'objet **Main System Chassis/Main System** (Châssis de système principal/Système principal) comprend les éléments suivants :

Propriétés

Sous-onglets : Health | Information | System Components (FRU) | Front Panel (Intégrité | Informations | Composants du système (FRU)| Panneau avant)

Sous l'onglet **Properties** (Propriétés), vous pouvez :

- Afficher l'intégrité ou la condition des composants matériels et des capteurs. Une icône System/Server Module Component Status Indicators (Voyants de condition du composant du système/module module du serveur) se trouve en regard du nom de chaque composant répertorié. indique que le composant est intègre (normal). indique que le composant a une condition d'avertissement (non critique) et qu'il doit être vérifié. indique que le

composant a une condition critique/défaillant et qu'il nécessite une intervention immédiate.  indique que la condition d'intégrité du composant est inconnue. Les composants surveillés disponibles comprennent :

- Batteries
- Ventilateurs
- Journal du matériel
- Intrusion
- Network (Réseau)
- Power Management (Gestion de l'alimentation)
- Blocs d'alimentation
- Processeurs
- Températures
- Tensions

REMARQUE : Les batteries sont prises en charge uniquement sur les systèmes Dell PowerEdge 9G et Dell PowerEdge 10G. Les **Power supplies** (Blocs d'alimentation) ne sont pas disponibles sur Dell PowerEdge 1900. La gestion de l'alimentation n'est prise en charge que sur un nombre limité de systèmes Dell PowerEdge 10G. Les fonctionnalités **Power Supply Monitoring** (Surveillance des blocs d'alimentation) et **Power Monitoring** (Surveillance de l'alimentation) sont uniquement disponibles pour les systèmes sur lesquels sont installés au moins deux blocs d'alimentation redondants remplaçables à chaud. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondant installés définitivement qui ne disposent pas de circuits de gestion de l'alimentation.

REMARQUE : Si l'adaptateur de bus hôte (HBA) Fibre Channel à port unique 4 Gb QLE2460 QLogic, le HBA Fibre Channel double port 4 Gb QLE2462 QLogic, l'adaptateur FC8 double port QLE2562 Qlogic, ou les cartes adaptateur FC8 à port unique QLE2560 Qlogic sont installées sur les systèmes 12G, l'écran **System Components (FRU)** (Composants du système (FRU)) ne s'affiche pas.

- Affichez des informations concernant les attributs du châssis de système principal tels que le nom d'hôte, la version iDRAC, la version du Lifecycle Controller, le modèle du châssis, le verrou du châssis, le numéro de service du châssis, le code de service express et le numéro d'inventaire du châssis. Le code de service express (ESC) est une conversion numérique (uniquement) de 11 chiffres du numéro de service du système Dell. Lorsque vous appelez le support technique Dell, vous pouvez taper le ESC pour acheminer automatiquement votre appel.
- Affichez des informations détaillées concernant les unités remplaçables sur site (FRU) installées sur votre système (sous le sous-onglet **System Components (FRU)** (Composants du système (FRU).)
- Activez ou désactivez les boutons du panneau avant du système géré, entre autres le bouton d'alimentation et le bouton NMI (Non-Masking Interrupt - Interruption non masquée) (s'il existe sur le système). Sélectionnez également le niveau d'accès de sécurité LCD du système géré. Utilisez le menu déroulant pour sélectionner les informations LCD du système géré. Vous pouvez également activer Indication of Remote KVM session (Indication d'une session KMV distante) dans le sous-onglet **Front Panel** (Panneau avant).

Batteries

Cliquez sur l'objet **Batteries** pour afficher les informations concernant les batteries installées sur votre système. Les batteries conservent l'heure et la date lorsque votre système est éteint. La batterie enregistre la configuration du BIOS du système, laquelle permet un bon redémarrage. La fenêtre d'action de l'objet Batteries peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties**, vous pouvez afficher les mesures actuelles et la condition des batteries de votre système.

Gestion des alertes

Sous l'onglet **Alert Management**, vous pouvez configurer les alertes que vous voulez activer en cas d'événement d'avertissement ou de panne/critique des batteries.

BIOS

Cliquez sur l'objet **BIOS** pour gérer les fonctions clés du BIOS de votre système. Le BIOS de votre système contient des programmes stockés sur un jeu de puces de la mémoire flash qui contrôle les communications entre le microprocesseur et les dispositifs périphériques, tels que le clavier et l'adaptateur vidéo, ainsi que d'autres fonctions, telles que les messages système. La fenêtre d'action de l'objet **BIOS** peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur :

Properties (Propriétés) et **Setup** (Configuration)

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties**, vous pouvez afficher les informations sur le BIOS.

Configuration

Sous-onglet : BIOS

REMARQUE : L'onglet Configuration du BIOS de votre système affiche uniquement les fonctionnalités du BIOS qui sont prises en charge sur votre système.

Sous l'onglet **Setup**, vous pouvez définir l'état des différents objets de configuration du BIOS.

Vous pouvez modifier la condition de la plupart des fonctions de configuration du BIOS, notamment mais sans s'y limiter, le port série, la séquence du disque dur, les ports USB accessibles par l'utilisateur, la technologie de virtualisation de l'UC, l'HyperThreading de l'UC, le mode de restauration de l'alimentation CA, le contrôleur SATA intégré, le profil du système, la redirection de la console, le débit en bauds à sécurité intégrée de la redirection de la console. Vous pouvez également configurer le périphérique USB interne, les paramètres du contrôleur du lecteur optique, le registre d'horloge de la surveillance ASR (automatic system recovery - restauration automatique du système), l'hyperviseur intégré et des ports de réseau LAN supplémentaires sur l'information de la carte mère. Vous pouvez également voir les paramètres TPM (Trusted Platform Module - Module de plateforme approuvée) et TCM (Trusted Cryptographic Module - Module cryptographique approuvé).

En fonction de la configuration spécifique du système, des éléments de configuration supplémentaires peuvent s'afficher. Cependant, certaines options de configuration du BIOS peuvent s'afficher sur l'écran de configuration du BIOS sans être pour autant accessibles dans Server Administrator.

Pour les systèmes 12G, les fonctions configurables du BIOS sont regroupées sous forme de catégories spécifiques. Les catégories incluent les informations système, les paramètres de mémoire, les paramètres du profil du système, les paramètres d'amorçage d'UEFI (Unified Extensible Firmware Interface - Interface micrologicielle extensible unifiée), les cartes NIC, l'amorçage ponctuel et la désactivation des emplacements. Par exemple, sur la page **System BIOS Settings** (Paramètres du BIOS du système), lorsque vous cliquez sur le lien **Memory Settings** (Paramètres de mémoire), les fonctions relatives à la mémoire système apparaissent. Vous pouvez afficher ou modifier les paramètres en navigant vers les catégories correspondantes.

Vous pouvez configurer un mot de passe de configuration du BIOS depuis la page **BIOS Setup - System Security** (Configuration BIOS - Sécurité du système). Vous devez saisir le mot de passe pour activer et modifier les paramètres du BIOS. Autrement, les paramètres du BIOS apparaissent en mode Lecture seule. Vous devez redémarrer le système suite à la définition du mot de passe.

Lorsque des valeurs en attente provenant d'une session précédente existent, ou lorsque la configuration intrabande est désactivée depuis une interface hors bande, Server Administrator interdit la configuration du BIOS.

REMARQUE : Les informations de configuration des NIC se trouvant dans la configuration du BIOS de Server Administrator peuvent êtres inexactes dans le cas de NIC intégrés. Utiliser l'écran de configuration du BIOS pour activer ou désactiver les NIC peut entraîner des résultats inattendus. Nous vous recommandons d'effectuer toutes les configurations des NIC intégrés via l'écran de configuration du système, disponible lorsque vous appuyez sur <F2> pendant l'amorçage d'un système.

Ventilateurs

Cliquez sur l'objet **Fans** (Ventilateurs) pour gérer les ventilateurs de votre système. Server Administrator surveille la condition de chaque système en mesurant les tours par minute des ventilateurs. Les capteurs de ventilateur rapportent les tours par minute au service Server Administrator Instrumentation Service. Lorsque vous sélectionnez Fans dans l'arborescence de périphériques, des détails apparaissent dans la zone de données du panneau de droite de la page d'accueil de Server Administrator. La fenêtre d'action de l'objet Fans peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

Propriétés

Sous-onglet : Fan Probes (Capteurs de ventilateurs)

Sous l'onglet **Properties** (Propriétés), vous pouvez :

- Afficher les mesures actuelles des capteurs des ventilateurs du système et configurer les valeurs minimales et maximales des seuils d'avertissement des capteurs des ventilateurs.

REMARQUE : Certains champs de capteur de ventilateur varient en fonction du type de micrologiciel de votre système, tel que BMC ou ESM. Certaines valeurs de seuil ne sont pas modifiables sur des systèmes BMC.

- Sélectionner les options de contrôle des ventilateurs.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet **Alert Management**, vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un ventilateur donne une valeur d'avertissement ou de panne.
- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux des seuils d'alerte des ventilateurs. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Micrologiciel

Cliquez sur l'objet **Firmware** (Micrologiciel) pour gérer le micrologiciel de votre système. Le micrologiciel est composé de programmes ou de données qui ont été écrites sur la mémoire morte (ROM). Le micrologiciel peut démarrer et opérer un périphérique. Chaque contrôleur contient un micrologiciel qui aide à fournir la fonctionnalité du contrôleur. La fenêtre d'action de l'objet **Firmware** (Micrologiciel) peut comporter l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés).

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties** (Propriétés), vous pouvez afficher les informations sur le micrologiciel du système.

Performances matérielles

Cliquez sur l'objet **Hardware Performance** (Performances matérielles) pour afficher la condition et la cause de la dégradation des performances du système. La fenêtre d'action de l'objet **Hardware Performance** peut comporter l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés).

Le tableau suivant répertorie les valeurs possibles pour la condition et la cause de la condition d'un capteur :

Tableau 9. Valeurs possibles pour la condition et la cause d'un capteur

Valeurs de condition	Valeurs de cause
Dégradé	Configuration de l'utilisateur Capacité d'alimentation insuffisante Raison inconnue
Normal	s.o.

- **Propriétés**
- **Sous-onglet : Informations**

Sous l'onglet **Properties** (Propriétés), vous pouvez afficher les détails de la dégradation des performances du système.

Intrusion

Cliquez sur l'objet **Intrusion** pour gérer la condition de l'intrusion dans le châssis de votre système. Server Administrator surveille la condition de l'intrusion dans le châssis. Il s'agit d'une mesure de sécurité pour protéger contre un accès non autorisé aux composants essentiels de votre système. L'intrusion dans châssis indique si quelqu'un ouvre ou a ouvert le cache du châssis du système. La fenêtre d'action de l'objet **Intrusion** peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes

Propriétés

Sous-onglet : Intrusion

Sous l'onglet **Properties**, vous pouvez afficher la condition de l'intrusion dans le châssis.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet **Alert Management**, vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un capteur d'intrusion donne une valeur d'avertissement ou de panne.
- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux de seuil d'alerte pour le capteur d'intrusion. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Mémoire

Cliquez sur l'objet **Memory** (Mémoire) pour gérer les périphériques de mémoire du système. Server Administrator surveille la condition du périphérique de mémoire de chaque module présent sur le système géré. Les capteurs d'échec anticipé des périphériques de mémoire surveillent les modules de mémoire en comptant le nombre de corrections de mémoire ECC. Server Administrator surveille également les informations de redondance de mémoire si votre système prend en charge cette fonction. La fenêtre d'action de l'objet **Memory** (Mémoire) peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

Propriétés

Sous-onglet : Memory (Mémoire)

Sous l'onglet **Properties** (Propriétés), vous pouvez voir la condition de redondance de la mémoire, les attributs de la matrice de mémoire, la capacité totale des matrices de mémoire, les détails des matrices de mémoire, les détails des périphériques de mémoire et la condition des périphériques de mémoire. Les détails des périphériques de mémoire offres des informations détaillées sur un connecteur telles que sa condition, le nom du périphérique, sa taille, son type, son rang et ses échecs. Un rang est une rangée de périphériques DRAM (dynamic random access memory - mémoire d'accès aléatoire dynamique) comprenant 64 bits de données par DIMM (Module de mémoire à connexion double). Les valeurs de rang possibles sont `unique`, `double`, `quadruple`, `octal`, et `hexa`. Le rang affiche le rang de la barrette DIMM et aide à maintenir facilement les DIMM du serveur.

REMARQUE : Si un système sur lequel une mémoire de rechange est activée perd sa redondance, il n'est pas certain de pouvoir déterminer quel module de mémoire est en cause. Si vous ne pouvez pas déterminer quelle barrette DIMM vous devez remplacer, consultez l'entrée de journal *switch to spare memory bank detected* (passer à la mémoire de rechange détectée) du journal système ESM pour découvrir quel module de mémoire est défaillant.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet **Alert Management** (Gestion des alertes), vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un module de mémoire donne une valeur d'avertissement ou de panne.
- Afficher les seuils d'alertes d'interruptions SNMP et définir les niveaux des seuils d'alerte des modules de mémoire. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Network (Réseau)

Cliquez sur l'objet **Network** (Réseau) pour gérer les NIC de votre système. Server Administrator surveille la condition de chaque NIC se trouvant dans votre système pour assurer une connexion distante continue. Dell OpenManage Server Administrator rapporte les capacités FCoE et iSoE des NIC. Les détails de regroupement des NIC sont également rapportés s'ils sont déjà configurés sur le système. Deux NIC ou plus peuvent être regroupés en un NIC logique unique, auquel un administrateur peut attribuer une adresse IP. Le regroupement peut être configuré à l'aide des outils du fournisseur NIC. Par exemple, Broadcom - BACS. Si l'un des NIC physique échoue, l'adresse IP reste accessible car elle est liée au NIC logique au lieu d'un NIC physique unique. Si l'interface de regroupement est configurée, les propriétés de regroupement détaillées sont affichées. La relation entre les NIC physiques et l'interface de regroupement (et vice-versa) est également rapportée, si ces NIC physiques sont membres de l'interface de regroupement.

Sur le système d'exploitation Windows 2008 Hypervisor, Server Administrator ne signale pas les adresses IP des ports NIC physiques utilisés pour attribuer une adresse IP à une machine virtuelle.

REMARQUE : Il n'est pas garanti que l'ordre dans lequel les périphériques sont détectés corresponde à l'ordre des ports physiques du périphérique. Cliquez sur l'hyperlien en dessous du nom de l'interface pour afficher les informations des NIC.

Si vous disposez de systèmes d'exploitation ESX et ESXi, le périphérique réseau est considéré comme un groupe. Par exemple, l'interface Ethernet virtuelle qui est utilisée par la console de services (vswif) et l'interface réseau virtuelle qui est utilisée par les périphériques VMKernel (vmknic) sur ESX et le périphérique vmknic sur ESXi.

La fenêtre d'action de l'objet **Network** (Réseau) peut comporter l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Properties** (Propriétés).

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties**, vous pouvez afficher les informations relatives aux interfaces NIC physiques, ainsi qu'aux interfaces de groupe, installées sur votre système.

REMARQUE : Dans la section IPv6 Addresses (Adresses IPv6), Server Administrator affiche uniquement deux adresses, en plus de l'adresse locale du lien.

Ports

Cliquez sur l'objet **Ports** pour gérer les ports externes de votre système. Server Administrator surveille la condition de chaque port externe présent sur votre système.

REMARQUE : Les ports USB du CMC reliés à l'aide des serveurs Lame ne sont pas énumérés par OMSA.

La fenêtre d'action de l'objet **Ports** peut avoir l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Properties** (Propriétés).

Sous-onglet : Informations

Propriétés

Sous l'onglet **Properties**, vous pouvez afficher les informations sur les ports internes et externes de votre système.

Power Management (Gestion de l'alimentation)

REMARQUE : Les fonctions Power Supply Monitoring (Surveillance des blocs d'alimentation) et Power Monitoring (Surveillance de l'alimentation) sont disponibles uniquement sur les systèmes sur lesquels sont installés au moins deux blocs d'alimentation redondants remplaçables à chaud. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondants installés de manière permanente qui ne disposent pas de circuits de gestion de l'alimentation.

Surveillance

Sous-onglets : Consumption | Statistics (Consommation | Statistiques)

Dans l'onglet **Consumption** (Consommation), vous pouvez afficher et gérer les informations relatives à la consommation électrique de votre système, en watts et BTU/h.

BTU/h = watt X 3,413 (valeur arrondie au nombre entier le plus proche)

Server Administrator surveille la condition de consommation électrique et l'ampérage, et suit les détails des statistiques d'alimentation.

Vous pouvez également voir System Instantaneous Headroom (Hauteur instantanée du système) et System Peak Headroom (Hauteur maximale du système). Les valeurs s'affichent en Watts et BTU/h (British Thermal Unit - Unité thermique britannique). Les seuils d'alimentation peuvent être définis en Watts et BTU/h.

L'onglet Statistics (Statistiques) vous permet d'afficher et de réinitialiser les statistiques de consommation de puissance de votre système comme la consommation énergétique, la puissance système maximale et l'intensité système maximale.

Gestion

Sous-onglets : Budget | Profiles (Bilan | Profils)

L'onglet **Budget** (Bilan) vous permet de voir les attributs de Power Inventory (Inventaire de l'alimentation) tels que System Idle Power (Alimentation inactive du système) et System Maximum Potential Power (Alimentation maximum potentielle du système) en Watt et BTU/h. Vous pouvez également utiliser l'option Power Budget (Bilan de l'alimentation) pour activer option Power Cap (Alimentation maximale) et définir l'alimentation maximale pour votre système.

L'onglet **Profiles** (Profils) vous permet de sélectionner un profil de puissance afin de maximiser les performances de votre système et de préserver l'énergie.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Utilisez l'onglet **Alert Actions** (Actions d'alerte) pour définir les actions d'alerte du système pour divers événements système, comme l'avertissement du capteur de puissance du système et la puissance système maximale.

Utilisez l'onglet **SNMP Traps** (Interruptions SNMP) pour configurer les interruptions SNMP de votre système.

Certaines fonctionnalités de gestion de l'alimentation sont uniquement disponibles sur les systèmes activés avec le bus de gestion de l'alimentation (PMBus).

Blocs d'alimentation

Cliquez sur l'objet **Power Supplies** (Blocs d'alimentation) pour gérer les blocs d'alimentation de votre système. Server Administrator surveille la condition des blocs d'alimentation, notamment la redondance, pour assurer que chaque bloc d'alimentation présent sur votre système fonctionne correctement. La fenêtre d'action de l'objet Power Supplies peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

REMARQUE : Les fonctions Power Supply Monitoring (Surveillance des blocs d'alimentation) et Power Monitoring (Surveillance de l'alimentation) sont disponibles uniquement sur les systèmes sur lesquels sont installés au moins deux blocs d'alimentation redondants remplaçables à chaud. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondants installés de manière permanente qui ne disposent pas de circuits de gestion de l'alimentation.

Propriétés

Sous-onglet : Elements (Éléments)

Sous l'onglet **Properties** (Propriétés), vous pouvez :

- Voir les informations sur les attributs de redondance de vos blocs d'alimentation.
- Vérifiez la condition des éléments individuels des blocs d'alimentation, notamment la version du micrologiciel du bloc d'alimentation, la tension d'entrée nominale et la tension de sortie maximale. L'attribut Rated Input Wattage (Tension d'entrée nominale) s'affiche uniquement sur les systèmes PMBus commençant par 11G.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet Alert Management (Gestion des alertes), vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si une alimentation du système donne une valeur d'avertissement ou de panne.
- Configurer les destinations des alertes d'événements sur plateforme pour les adresses IPv6.
- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux des seuils d'alerte pour l'alimentation système en watt. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

REMARQUE : L'interruption System Peak Power (Puissance système maximale) génère des événements uniquement pour indiquer la gravité.

Processeurs

Cliquez sur l'objet **Processors** (Processeurs) pour gérer les microprocesseurs de votre système. Un processeur est la puce de calcul principal d'un système qui contrôle l'interprétation et l'exécution des fonctions arithmétiques et logiques. La fenêtre d'action de l'objet Processors peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

Sous-onglet : Informations

Propriétés

Sous l'onglet **Properties**, vous pouvez afficher des informations sur les microprocesseurs de votre système et accéder à des informations détaillées sur les capacités et le cache.

Gestion des alertes

Sous-onglets : Alert Actions (Actions d'alerte)

Sous l'onglet **Alert Management** (Gestion des alertes), vous pouvez afficher les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un processeur renvoie une valeur d'avertissement ou de panne.

Accès à distance

Cliquez sur l'objet **Remote Access** (Accès à distance) pour gérer les fonctionnalités Baseboard Management Controller (BMC) ou Integrated Dell Remote Access Controller (iDRAC), et les fonctionnalités Remote Access Controller.

La sélection de l'onglet Remote Access vous permet de gérer les fonctionnalités du BMC/iDRAC, telles que les informations générales sur le BMC/iDRAC. Vous pouvez également gérer la configuration du BMC/iDRAC sur un réseau LAN, du port série du BMC/iDRAC, des paramètres du mode terminal du port série, du BMC/iDRAC sur une connexion série sur LAN, et des utilisateurs BMC/iDRAC.

REMARQUE : Le contrôleur BMC est pris en charge sur les systèmes Dell PowerEdge 9G et le contrôleur iDRAC est pris en charge sur les systèmes Dell 10G et 11x uniquement.

REMARQUE : Si une application autre que Server Administrator est utilisée pour configurer le BMC/iDRAC alors que Server Administrator est en cours d'exécution, les données de configuration du BMC/iDRAC affichées par Server Administrator peuvent devenir asynchrones avec le BMC/iDRAC. Nous vous recommandons d'utiliser Server Administrator pour configurer le BMC/iDRAC lorsque Server Administrator est en cours d'exécution.

Le contrôleur DRAC vous permet d'accéder aux capacités de gestion du système à distance de votre système. Le DRAC de Server Administrator fournit un accès à distance aux systèmes inopérants, vous avertit lorsqu'un système ne fonctionne plus et a la capacité de redémarrer un système.

La fenêtre d'action de l'objet **Remote Access** (Accès à distance) peut présenter les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Properties** (Propriétés), **Configuration** et Users (Utilisateurs).

Sous-onglet : Informations

Propriétés

Sous l'onglet **Properties** (Propriétés), vous pouvez consulter des informations générales sur le périphérique d'accès à distance. Vous pouvez également y consulter les attributs des adresses IPv4 et IPv6.

Cliquez sur **Reset to Defaults** (Restaurer les valeurs par défaut) pour réinitialiser tous les attributs sur leurs valeurs système par défaut.

Sous-onglets : LAN | Serial Port | Serial Over LAN | Additional Configuration (Réseau LAN | Port série | Connexion série sur le réseau LAN |Configuration supplémentaire)

Configuration

Sous l'onglet Configuration, lorsque le BMC/iDRAC est configuré, vous pouvez configurer le BMC/iDRAC sur un réseau LAN, le port série du contrôleur BMC/iDRAC et les connexions série sur le réseau LAN du BMC/iDRAC.

REMARQUE : L'onglet Additional configuration (Configuration supplémentaire) est disponible uniquement sur les systèmes dotés du contrôleur iDRAC.

Sous l'onglet **Configuration**, lorsque le DRAC est configuré, vous pouvez configurer des propriétés de réseau :

REMARQUE : Les champs Enable NIC (Activer la NIC), NIC Selection (Sélection de NIC) et Encryption Key (Clé de cryptage) ne s'affichent que sur les systèmes Dell PowerEdge 9G.

Sous l'onglet **Additional Configuration** (Configuration supplémentaire), vous pouvez activer ou désactiver les propriétés IPv4/IPv6.

REMARQUE : L'activation ou la désactivation d'IPv4/IPv6 est possible uniquement dans un environnement bipile (au sein duquel les piles IPv4 et IPv6 sont chargées).

Utilisateurs

Sous-onglet : Users (Utilisateurs)

Sous l'onglet **Users** (Utilisateurs), vous pouvez modifier la configuration de l'utilisateur pour l'accès à distance. Vous pouvez ajouter, configurer et afficher des informations sur les utilisateurs RAC (Remote Access Controller).

REMARQUE : Sur les systèmes Dell PowerEdge 9G :

- Dix ID utilisateur sont affichés. Si une carte DRAC est installée, seize ID utilisateur sont affichés.
- La colonne Serial Over LAN Payload (Charge utile des communications série sur le LAN) s'affiche.

Média flash amovible

Cliquez sur l'objet **Removable Flash Media** (Média flash amovible) pour afficher la condition d'intégrité et de redondance des modules SD internes et du média vFlash. La fenêtre d'action de l'objet Removable Flash Media comporte l'onglet **Properties** (Propriétés).

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties**, vous pouvez afficher des informations concernant le média flash amovible et les modules SD internes. Cela inclut des informations détaillées concernant le nom du connecteur, sa condition et sa taille de stockage.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet **Alert Management**, vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si le capteur du média flash amovible retourne une valeur d'avertissement ou de panne.
- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux de seuil d'alerte pour les capteurs du média flash amovible. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Alert management est commun pour les modules SD internes et vFlash. Configurer des actions d'alerte/SNMP/PEF pour les modules SD ou vFlash les configure automatiquement pour l'autre.

Logements

Cliquez sur l'objet **Slots** (Logements) pour gérer les connecteurs ou sockets de votre carte système qui acceptent les cartes de circuits imprimés, telles que les cartes d'extension. La fenêtre d'action de l'objet Slots comporte l'onglet **Properties** (Propriétés).

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties**, vous pouvez afficher des informations sur tous les logements et toutes les cartes installées.

Températures

Cliquez sur l'objet **Temperatures** (Températures) pour gérer la température de votre système afin d'éviter tout dommage thermique aux composants internes de votre système. Server Administrator surveille la température dans divers emplacements du châssis de votre système pour assurer que les températures à l'intérieur du châssis ne soient pas trop élevées. La fenêtre d'action de l'objet **Temperatures** affiche les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

Sous-onglet : Temperature Probes (Capteurs de température)

Propriétés

-
-

Sous l'onglet **Properties**, vous pouvez consulter les mesures actuelles et les conditions des capteurs de température de votre système, et configurer les valeurs minimale et maximale du seuil d'avertissement des capteurs de température.

REMARQUE : Certains champs de capteurs de température varient en fonction du type de micrologiciel de votre système, tels que BMC ou ESM. Certaines valeurs de seuils ne sont pas modifiables sur des systèmes BMC. Lors de l'attribution de valeurs de seuils aux capteurs, il arrive que Server Administrator arrondisse les valeurs maximales ou minimales à la valeur attribuable la plus proche.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet **Alert Management** (Gestion des alertes), vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un capteur de température renvoie une valeur d'avertissement ou de panne.
- Afficher les seuils d'alerte des interruptions SNMP et définir les niveaux de seuils d'alerte des capteurs de température. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

REMARQUE : Vous pouvez définir les valeurs de seuil des capteurs de température d'un châssis externe sur des nombres entiers uniquement. Si vous tentez de définir une valeur de seuil de capteur de température sur un nombre contenant une décimale, seul le nombre entier avant la décimale sera enregistré en tant que paramètre de seuil.

Tensions

Cliquez sur l'objet **Voltages** (Tensions) pour gérer les niveaux de tension dans votre système. Server Administrator surveille les tensions de divers composants critiques dans divers emplacements du châssis du système surveillé. La fenêtre d'action de l'objet **Voltages** peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés) et **Alert Management** (Gestion des alertes).

Propriétés

Sous-onglet : Voltage Probes (Capteurs de tension)

Sous l'onglet **Properties** (Propriétés), vous pouvez consulter les mesures actuelles et les conditions des capteurs de tension de votre système, et configurer les valeurs minimale et maximale du seuil d'avertissement des capteurs de tension.

REMARQUE : Certains champs des capteurs de tension varient en fonction du type de micrologiciel de votre système, tel que BMC ou ESM. Certaines valeurs de seuil ne sont pas modifiables sur des systèmes BMC.

Gestion des alertes

Sous-onglets : Alert Actions | SNMP Traps (Actions d'alerte | Interruptions SNMP)

Sous l'onglet **Alert Management** (Gestion des alertes), vous pouvez :

- Afficher les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un capteur de tension du système renvoie une valeur d'avertissement ou de panne.
- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux de seuil d'alerte pour les capteurs de tension. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Logiciels

Cliquez sur l'objet **Software** (Logiciels) pour afficher des informations détaillées sur la version des composants logiciels essentiels du système, tels que le système d'exploitation et le logiciel de gestion de systèmes. La fenêtre d'action de l'objet Software (Logiciels) comporte l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés).

Sous-onglet : Summary (Résumé)

Propriétés

Sous l'onglet **Properties** (Propriétés), vous pouvez afficher un résumé du système d'exploitation et du logiciel de gestion de systèmes du système surveillé.

Système d'exploitation

Cliquez sur l'objet **Operating System** (Système d'exploitation) pour afficher des informations de base sur votre système d'exploitation. La fenêtre d'action de l'objet Operating System comporte l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Properties** (Propriétés).

Propriétés

Sous-onglet : Informations

Sous l'onglet **Properties**, vous pouvez afficher des informations de base sur votre système d'exploitation.

Stockage

Server Administrator fournit un service de gestion du stockage (Storage Management Service) :

Le Storage Management Service fournit des fonctions permettant la configuration de périphériques de stockage. Dans certains cas, le Storage Management Service est installé à l'aide de **Typical Setup** (Configuration typique). Le Storage Management Service est disponible sur les systèmes d'exploitation Microsoft Windows, Red Hat Enterprise Linux et SUSE Linux Enterprise Server.

Lorsque Storage Management Service est installé, cliquez sur l'objet **Storage** (Stockage) pour afficher la condition et les paramètres des divers périphériques de stockage de matrice reliés, des disques système, etc.

Pour Storage Management Service, la fenêtre d'action de l'objet Storage comporte l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Properties**.

Propriétés

Sous-onglet : Health (Intégrité)

Sous l'onglet **Properties**, vous pouvez afficher l'intégrité ou la condition des composants de stockage et des capteurs connectés, par exemple, les sous-systèmes de matrice et les disques du système d'exploitation.

Gestion des préférences : Options de configuration de la page d'accueil

Le panneau gauche de la page d'accueil **Preferences** (Préférences) (où l'arborescence système s'affiche sur la page d'accueil de Server Administrator) affiche toutes les informations de configuration disponibles dans la fenêtre de l'arborescence système. Les options affichées sont basées sur le logiciel de gestion des systèmes installé sur le système géré.

Les options de configuration disponibles de la page d'accueil **Preferences** (Préférences) sont les suivantes :

- Paramètres généraux
- Server Administrator

Paramètres généraux

Cliquez sur l'objet **General Settings** (Paramètres généraux) pour définir les préférences utilisateur et du service DSM SA Connection Service (Web Server) pour les fonctions Server Administrator sélectionnées. La fenêtre d'action de l'objet General Settings comporte les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **User** (Utilisateur) et **Web Server**.

Sous-onglet : Properties (Propriétés)

Utilisateur

Sous l'onglet **User** (Utilisateur), vous pouvez définir les préférences de l'utilisateur, comme l'apparence de la page d'accueil et l'adresse e-mail par défaut pour le bouton **E-mail**.

- **Web Server**
- **Sous-onglets : Properties | X.509 Certificate (Propriétés | Certificat X.509)**

Sous l'onglet Web Server, vous pouvez :

- Définir les préférences du service DSM SA Connection Service. Pour des instructions pour configurer les préférences du serveur, voir Dell Systems Dell Systems Management Server Administration Connection Service and Security Setup (Configuration du service Dell Systems Management Server Administration Connection Service et de la sécurité des systèmes Dell).
- Configurer l'adresse de serveur SMTP et l'adresse IP de liaison dans le mode d'adressage IPv4 ou IPv6.
- Gérez les certificats X.509 en générant un nouveau certificat X.509, en réutilisant un certificat X.509 existant, ou en important un certificat racine ou une chaîne de certificat depuis une autorité de certification (CA). Pour en savoir plus sur la gestion des certificats, voir Gestion des certificats X.509.

Server Administrator

Cliquez sur l'objet **Server Administrator** pour autoriser ou interdire l'accès aux utilisateurs dotés de privilèges d'utilisateur ou d'utilisateur privilégié et pour configurer le mot de passe racine SNMP. La fenêtre d'action de l'objet **Server Administrator** peut comporter l'onglet suivant, selon les privilèges du groupe de l'utilisateur : **Preferences** (Préférences).

Sous-onglets : Access Configuration | SNMP Configuration (Configuration de l'accès | Configuration SNMP)

Préférences

Sous l'onglet **Preferences** (Préférences), vous pouvez :

- Autoriser ou interdire l'accès aux utilisateurs dotés de privilèges d'utilisateur ou d'utilisateur privilégié
- Configurer le mot de passe racine SNMP.

  REMARQUE : L'utilisateur par défaut pour la configuration SNMP est l'utilisateur root (racine) et le mot de passe est calvin.
- Configurer les opérations Set SNMP.

  REMARQUE : Après avoir configuré les opérations Set SNMP, vous devez redémarrer les services pour que la modification prenne effet. Sur les systèmes exécutant des systèmes d'exploitation Windows Microsoft pris en charge, le service SNMP Windows doit être redémarré. Sur les systèmes exécutant des systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge, les services Server Administrator doivent être redémarrés à l'aide de la commande de redémarrage `srvadmin-services.sh`.

5

Utilisation de Remote Access Controller

Ce chapitre fournit des informations relatives à l'accès aux fonctionnalités d'accès à distance des contrôleurs BMC/ iDRAC et DRAC, et à leur utilisation.

Le BMC (baseboard management controller)/iDRAC (Integrated Dell Remote Access Controller) de systèmes Dell surveille le système et détecte les événements critiques en communiquant avec divers capteurs de la carte système et en envoyant des alertes et des événements de journal lorsque certains paramètres dépassent leurs seuils prédéfinis. Le BMC/iDRAC prend en charge la spécification IPMI (Intelligent Platform Management Interface) de norme d'entreprise, vous permettant de configurer, surveiller et restaurer les systèmes à distance.

REMARQUE : Le contrôleur BMC (Baseboard management controller - Gestion de carte mère) est pris en charge par les systèmes Dell PowerEdge 9G et le contrôleur iDRAC (Integrated Dell Remote Access Controller -Contrôleur d'accès à distance Dell intégré) est pris en charge par les systèmes Dell PowerEdge 10G et 11G.

Le DRAC est une solution matérielle et logicielle de gestion de systèmes, conçue pour fournir des capacités de gestion à distance, de remise en état d'un système suite à une panne et de contrôle de l'alimentation pour les systèmes Dell.

En communiquant avec le contrôleur BMC (baseboard management controller)/ iDRAC (Integrated Dell Remote Access Controller) du système, le DRAC peut être configuré pour vous envoyer des alertes par e-mail d'avertissement ou d'erreur concernant les tensions, les températures et les vitesses de ventilateur. Le DRAC journalise également les données d'événements et l'écran de panne le plus récent (disponible uniquement sur des systèmes exécutant un système d'exploitation Microsoft Windows) pour vous aider à diagnostiquer la cause probable d'une panne du système.

Le Remote Access Controller fournit un accès à distance à un système inopérant, vous permettant de rétablir ce système dès que possible. Le Remote Access Controller fournit également une notification d'alerte lorsqu'un système est en panne et vous permet de redémarrer un système à distance. En outre, le Remote Access Controller journalise la cause probable des plantages d'un système et enregistre *l'écran de panne le plus récent*.

Vous pouvez ouvrir une session sur Remote Access Controller à partir de la page d'accueil de Server Administrator ou en accédant directement à l'adresse IP du contrôleur avec un navigateur pris en charge.

Lorsque vous utilisez le Remote Access Controller, vous pouvez cliquer sur **Help** (Aide) pour obtenir des informations détaillées concernant la fenêtre spécifique sur laquelle vous vous trouvez. L'aide du Remote Access Controller est disponible pour toutes les fenêtres auquelles l'utilisateur a accès, en fonction des privilège dont il dispose et des groupes matériels et logiciels spécifiques que Server Administrator découvre sur le système géré.

REMARQUE : Pour en savoir plus sur le BMC, voir le *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Guide d'utilisation des utilitaires du Dell OpenManage Baseboard Management Controller) à l'adresse **dell.com/support/manuals**.

REMARQUE : Pour en savoir plus sur l'utilisation de DRAC 5, voir le *Dell Remote Access Controller 5 User's Guide* (Guide d'utilisation du Dell Remote Access Controller 5) à l'adresse **dell.com/support/manuals**.

REMARQUE : Pour des informations détaillées sur la configuration et l'utilisation de l'iDRAC, voir le *Integrated Dell Remote Access Controller User's Guide* (Guide de l'utilisation de l'Integrated Dell Remote Access Controller) à l'adresse **dell.com/support/manuals**.

Le tableau suivant répertorie les noms des champs de l'interface utilisateur graphique (IUG) et le système applicable, lorsque Server Administrator est installé sur le système.

Tableau 10. Noms des champs de l'interface utilisateur graphique et du système applicable

Nom de champ de l'interface utilisateur graphique	Système concerné
Enceinte modulaire	Système modulaire
Modules de serveur	Système modulaire
Système principal	Système modulaire
Système	Système non-modulaire
Châssis principal du système	Système non-modulaire

Pour en savoir plus sur la prise en charge de périphériques d'accès à distance par le système, voir la *Dell Systems Software Support Matrix* (Matrice de prise en charge logicielle des systèmes Dell) disponible à l'adresse **dell.com/support/manuals**.

Server Administrator offre un accès distant intrabande aux journaux des événements, contrôle de l'alimentation et informations de condition des capteurs, et permet de configurer le BMC/iDRAC. Pour gérer le BMC/iDRAC et le DRAC via l'interface utilisateur graphique (IUG) de Server Administrator, cliquez sur l'objet **Remote Access** (Accès à distance), lequel est un sous-composant du groupe **Main System Chassis/Main System** (Châssis de système principal/Système principal).

Vous pouvez réaliser les tâches suivantes :

- Affichage des informations de base
- Configuration du périphérique d'accès à distance pour utiliser une connexion LAN
- Configuration du périphérique d'accès à distance pour utiliser une communication série sur le LAN
- Configuration du périphérique d'accès à distance pour utiliser une connexion par port série
- Configuration supplémentaire pour iDRAC
- Configuration des utilisateurs du périphérique d'accès à distance
- Définition des alertes de filtre d'événements sur plateforme

Vous pouvez consulter les informations sur le contrôleur BMC/iDRAC ou DRAC en fonction du matériel qui fournit les capacités d'accès à distance du système.

Le compte-rendu et la configuration des contrôleurs BMC/iDRAC et DRAC peuvent également être gérés à l'aide de la commande CLI `omreport/omconfig chassis remoteaccess`.

De plus, vous pouvez utiliser Server Administrator Instrumentation Service pour gérer les paramètres de filtres d'événements sur plate-forme (PEF) et les destinations d'alerte.

REMARQUE : Vous pouvez consulter les données du contrôleur BMC sur les systèmes Dell PowerEdge 9G uniquement.

Affichage des informations de base

Vous pouvez afficher des informations de base concernant le BMC/iDRAC, l'adresse IPv4 et le DRAC. Vous pouvez également réinitialiser les paramètres du contrôleur d'accès à distance à leurs valeurs par défaut. Pour ce faire :

REMARQUE : Vous devez être connecté avec des privilèges d'administrateur pour pouvoir réinitialiser les paramètres du contrôleur BMC.

Cliquez sur **Modular Enclosure** → **System/Server Module** → **Main System Chassis/Main System** → **Remote Access** (Enceinte Modulaire > Système/Module du serveur > Châssis de système principal/Système principal > Accès à distance)

La page **Remote Access** affiche les informations essentielles suivantes sur le contrôleur BMC de votre système :

Périphérique d'accès à distance

- Type de périphérique
- Version IPMI
- GUID système
- Nombre de sessions actives possibles
- Nombre de sessions actives
- LAN activé
- SOL activé
- Adresse MAC

Adresse IPv4

- Source d'adresse IP
- Adresse IP :
- Sous-réseau IP
- Passerelle IP

Adresse IPv6

- Source d'adresse IP
- Adresse IPv6 1
- Passerelle par défaut
- Adresse IPv6 2
- Adresse locale de liaison
- Source d'adresse DNS
- Serveur DNS préféré
- Serveur DNS auxiliaire

REMARQUE : Vous pouvez afficher les détails relatifs aux adresses IPv4 et IPv6 uniquement si vous activez les propriétés d'adresses IPv4 et IPv6 sous **Additional Configuration** (Configuration supplémentaire) dans l'onglet **Remote Access**.

Configuration du périphérique d'accès à distance pour utiliser une connexion LAN

Pour configurer le périphérique d'accès à distance en vue d'établir une communication sur un LAN :

1. Cliquez sur l'objet **Modular Enclosure → System/Server Module → Main System Chassis/Main System → Remote Access** (Enceinte Modulaire > Système/Module du serveur > Châssis de système principal/Système principal > Accès à distance).
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **LAN**.

   La fenêtre **LAN Configuration** (Configuration du LAN) s'affiche.

   REMARQUE : Le trafic de gestion des contrôleurs BMC/iDRAC ne fonctionne pas correctement si le réseau local sur carte mère (LOM) est regroupé avec des cartes d'extension d'adaptateur réseau.
4. Spécifiez les détails de configuration du NIC suivants :

- Enable NIC (Activer le NIC) (Cette option est disponible sur les systèmes Dell PowerEdge 9G lorsque le DRAC est installé. Sélectionnez-la pour le regroupement de NIC. Dans les systèmes Dell PowerEdge 9G, vous pouvez regrouper les NIC pour obtenir davantage de redondance.)

REMARQUE : Votre DRAC contient un NIC Ethernet 10BASE-T/100BASE-T intégré et prend en charge TCP/IP. Le NIC possède une adresse par défaut (192.168.20.1) et une passerelle par défaut (192.168.20.1).

REMARQUE : Si votre DRAC est configuré avec la même adresse IP qu'un autre NIC sur le même réseau, un conflit d'adresses IP se produit. Le DRAC ne répond alors plus aux commandes du réseau et ce jusqu'à ce que son adresse IP soit changée. Le DRAC doit être réinitialiser, même si le conflit d'adresses IP est résolu par la modification de l'adresse IP du NIC.

REMARQUE : Modifier l'adresse IP du DRAC entraîne la réinitialisation de ce dernier. Si le SNMP interroge le DRAC avant sa réinitialisation, un avertissement de température est journalisé, car la température n'est correctement communiquée qu'une fois le DRAC initialisé.

  - Sélection de NIC

REMARQUE : L'option NIC Selection (sélection de NIC) ne peut pas être configurée sur les systèmes modulaires.

REMARQUE : L'option Sélection de NIC est disponible sur les systèmes 11G et de version antérieure uniquement.

- Options de réseau principal et de basculement

Pour les systèmes 12G, les options de réseau principal pour le **NIC** d'accès à distance (iDRAC7) sont les suivantes : **LOM1**, **LOM2**, **LOM3**, **LOM4** et **Dedicated** (Dédié). Les options de réseau de basculement sont : **LOM1**, **LOM2**, **LOM3**, **LOM4**, **All LOMs** (Tous les LOM) et **None** (Aucun).

L'option Dedicated (Dédié) est disponible lorsque la licence iDRAC7 Enterprise License existe et est valide.

REMARQUE : Le nombre de LOM varie selon la configuration du système ou du matériel.

- Activer IPMI sur le LAN
- Source d'adresse IP
- Adresse IP :
- Masque de sous-réseau
- Adresse de passerelle
- Limite du niveau de privilège du canal
- New Encryption Key (Nouvelle clé de cryptage) (cette option est disponible sur les systèmes Dell PowerEdge 9G).

5. Spécifiez les détails suivants de la configuration du VLAN en option :

REMARQUE : La configuration du VLAN ne s'applique pas aux systèmes sur lesquels le contrôleur iDRAC est installé.

- Activer l'ID du VLAN
- ID du VLAN
- Priorité

6. Configurez les propriétés IPv4 suivantes :

- Source d'adresse IP
- Adresse IP :
- Masque de sous-réseau

- Adresse de passerelle

7. Configurez les propriétés IPv6 suivantes :

   - Source d'adresse IP
   - Adresse IP :
   - Longueur du préfixe
   - Passerelle par défaut
   - Source d'adresse DNS
   - Serveur DNS préféré
   - Serveur DNS auxiliaire

   REMARQUE : Vous êtes en mesure de configurer les détails relatifs aux adresses IPv4 et IPv6 uniquement si vous activez les propriétés IPv4 et IPv6 sous **Additional Configuration** (Configuration supplémentaire).

8. Cliquez sur **Appliquer les changements**.

Configuration du périphérique d'accès à distance pour utiliser une connexion par port série

Vous pouvez configurer le contrôleur BMC pour les communications sur un port série.

1. Cliquez sur **Modular Enclosure → System/Server Module → Main System Chassis/Main System → Remote Access** (Enceinte Modulaire > Système/Module du serveur > Châssis de système principal/Système principal > Accès à distance).
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Serial Port** (Port série).

   La fenêtre **Serial Port Configuration** (Configuration du port série) apparaît.

4. Configurez les détails suivants :

   - Paramètre du mode de connexion
   - Débit en bauds
   - Contrôle du débit
   - Limite du niveau de privilège du canal

5. Cliquez sur **Appliquer les changements**.
6. Cliquez sur **Terminal Mode Settings** (Paramètres du mode terminal).

   Dans la fenêtre Terminal Mode Settings (Paramètres du mode terminal), vous pouvez configurer les paramètres du mode terminal pour le port série.

   Le mode Terminal est utilisé pour l'envoi de messages IPMI (Intelligent Platform Interface Management) sur un port série avec des caractères ASCII imprimables. Le mode Terminal prend également en charge un nombre limité de commandes texte pour prendre en charge des environnement texte hérités. Cet environnement est conçu de manière à ce qu'un simple terminal ou émulateur de terminal peut être utilisé.

7. Spécifiez les personnalisations suivantes pour accroître la compatibilité avec les terminaux existants :

   - Modification de ligne
   - Contrôle de la suppression
   - Contrôle d'écho
   - Contrôle de la négociation
   - Nouvelle séquence linéaire
   - Saisie d'une nouvelle séquence linéaire

8. Cliquez sur **Appliquer les changements**.
9. Cliquez sur **Back To Serial Port Configuration Window** (Retourner à la fenêtre Configuration du port série) pour revenir à la fenêtre **Serial Port Configuration** (Configuration du port série).

Configuration du périphérique d'accès à distance pour utiliser une communication série sur le LAN

Pour configurer les contrôleurs BMC/iDRAC pour les communications série sur le réseau local (SOL) :

1. Cliquez sur l'objet **Modular Enclosure → System/Server Module → Main System Chassis/Main System → Remote Access** (Enceinte Modulaire > Système/Module du serveur > Châssis de système principal/Système principal > Accès à distance).
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Serial Over LAN** (Communications série sur le LAN).

   La fenêtre **Serial Over LAN Configuration** (Configuration de la connexion série sur le réseau local (LAN)) apparaît.
4. Configurez les détails suivants :

   - Activation des communications série sur le LAN
   - Débit en bauds
   - Minimum de privilèges requis
5. Cliquez sur **Appliquer les changements**.
6. Cliquez sur **Advanced Settings** (Paramètres avancés) pour configurer le contrôleur BMC.
7. Dans la fenêtre **Serial Over LAN Configuration Advanced Settings** (Paramètres avancés de la configuration de la connexion série sur le réseau local), vous pouvez spécifier les informations suivantes :

   - Intervalle d'accumulation des caractères
   - Seuil d'envoi des caractères
8. Cliquez sur **Appliquer les changements**.
9. Cliquez sur **Go Back to Serial Over LAN Configuration** (Retourner à la configuration de la connexion série sur le réseau local) pour revenir à la fenêtre **Serial Over LAN Configuration** (Configuration de la connexion série sur le réseau local).

Configuration supplémentaire pour iDRAC

Vous pouvez configurer les propriétés IPv4 et IPv6 via l'onglet **Additional Configuration** (Configuration supplémentaire).

1. Cliquez sur l'objet **Modular Enclosure→ System/Server Module → Main System Chassis/Main System→ Remote Access (Enceinte Modulaire > Système/Module du serveur > Châssis de système principal/Système principal > Accès à distance)**
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Additional Configuration**.
4. Configurez les propriétés IPv4 et IPv6 en les définissant sur **Enabled** (Activé) ou **Disabled** (Désactivé).
5. Cliquez sur **Appliquer les changements**.

REMARQUE : Pour en savoir plus sur la gestion des licences, voir le *Dell License Manager User's Guide* (Guide d'utilisation de Dell License Manager) disponible sur le site **dell.com/support/manuals**.

Configuration des utilisateurs du périphérique d'accès à distance

Pour configurer les utilisateurs du périphérique d'accès à distance à l'aide de la page Remote Access (Accès à distance) :

1. Cliquez sur l'objet **Modular Enclosure → System/Server Module → Main System Chassis/Main System → Remote Access** (Enceinte Modulaire > Système/Module du serveur > Châssis de système principal/Système principal > Accès à distance).
2. Cliquez sur l'onglet **Users** (Utilisateurs).

   La fenêtre **Remote Access Users** (Utilisateurs de l'accès à distance) affiche des informations sur les utilisateurs qui peuvent être configurés en tant qu'utilisateurs des contrôleurs BMC/iDRAC.
3. Cliquez sur **User ID** (ID d'utilisateur) pour configurer un nouvel utilisateur des contrôleurs BMC/iDRAC ou un utilisateur existant.

   La fenêtre **Remote Access User Configuration** (Configuration des utilisateurs de l'accès à distance) vous permet de configurer un utilisateur des contrôleurs BMC/iDRAC spécifique.
4. Spécifiez les informations générales suivantes :

   - Sélectionnez **Enable User** (Activer l'utilisateur) pour activer l'utilisateur.
   - Entrez le nom de l'utilisateur dans le champ **User Name** (Nom d'utilisateur).
   - Cochez la case **Change Password** (Modifier le mot de passe).
   - Entrez un nouveau mot de passe dans le champ **New Password** (Nouveau mot de passe).
   - Entrez de nouveau le nouveau mot de passe dans le champ **Confirm New Password** (Confirmer le nouveau mot de passe).
5. Spécifiez les privilèges d'utilisateur suivants :

   - Sélectionnez la limite maximale de privilèges utilisateur sur le réseau local.
   - Sélectionnez la limite maximale de privilèges utilisateur sur le port série accordée.
   - Sur les systèmes Dell PowerEdge 9G, sélectionnez **Enable Serial Over LAN** (Activer la fonction Série sur le LAN) pour activer cette fonction.
6. Spécifiez le groupe d'utilisateurs pour les privilèges d'utilisateur des contrôleurs DRAC/iDRAC.
7. Cliquez sur **Apply Changes** (Appliquer les modifications) pour enregistrer les modifications.
8. Cliquez sur **Back to Remote Access User Window** (Retour à la fenêtre Utilisateurs de l'accès à distance) pour retourner à la fenêtre **Remote Access Users** (Utilisateurs de l'accès à distance).

   REMARQUE : Six entrées utilisateur supplémentaires sont configurables lorsque le DRAC est installé. Ceci entraîne un total de 16 utilisateurs. Les mêmes règles de nom d'utilisateur et de mot de passe s'appliquent aux utilisateurs des BMC/iDRAC et RAC. Lorsque le DRAC/iDRAC6 est installé, les 16 entrées utilisateur sont allouées au DRAC.

Définition des alertes de filtre d'événements sur plateforme

Pour configurer les fonctionnalités BMC les plus pertinentes à l'aide du service Server Administrator Instrumentation, telles que les paramètres du filtre des événements sur plateforme (PEF) et les destinations d'alertes :

1. Cliquez sur l'objet **System** (Système).
2. Cliquez sur l'onglet **Management Alert** (Gestion des alertes).
3. Cliquez sur **Platform Events** (Événements sur plateforme).

   La fenêtre **Platform Events** vous permet de prendre des actions individuelles en réponse à des événements spécifiques de la plateforme. Vous pouvez sélectionner les événements pour lesquels vous souhaitez prendre des

actions d'arrêt et générer des alertes pour les actions sélectionnées. Vous pouvez également envoyer des alertes à des destinations d'adresses IP spécifiques de votre choix.

REMARQUE : Vous devez être connecté avec des privilèges d'administrateur pour pouvoir configurer les alertes des filtres d'événements sur plateforme (PEF) du contrôleur BMC.

REMARQUE : Le paramètre **Enable Platform Event Filters Alerts** (Activer les alertes des filtres d'événements sur plateforme) active ou désactive la génération d'alertes PEF. Il est indépendant des paramètres d'alertes d'événements de plateforme.

REMARQUE : Les paramètres System Power Probe Warning (Avertissement de capteur de puissance système) et **System Power Probe Failure** (Panne de capteur de puissance système) ne sont pas pris en charge par les systèmes Dell ne prenant pas en charge PMBus, bien que Server Administrator vous permette cette configuration.

REMARQUE : Sur les systèmes Dell PowerEdge 1900, les filtres d'événements de plateforme Avertissement de PS/VRM/D2D, Panne de PS/VRM/D2D et Bloc d'alimentation absent ne sont pas pris en charge, même si Server Administrator vous permet de configurer ces filtres d'événements.

4. Choisissez l'événement de plateforme pour lequel vous voulez effectuer des actions d'arrêt ou générer des alertes pour les actions sélectionnées et cliquez sur **Set Platform Events** (Définir des événements de plateforme).

   La fenêtre **Set Platform Events** (Définition d'événements sur plateforme) permet de spécifier les actions à entreprendre si le système doit être arrêté en réponse à un événement de plateforme.

5. Sélectionnez l'une des actions suivantes :

   - **Aucun**
   - **Redémarrer le système**

     Arrête le système d'exploitation et redémarre le système en effectuant les vérifications BIOS et en rechargeant le système d'exploitation.

   - **Arrêter le système**

     Coupe l'alimentation du système.

   - **Exécuter un cycle d'alimentation sur le système**

     Met hors tension l'alimentation électrique du système, marque une pause, met le système sous tension et le redémarre. Un cycle d'alimentation est utile lorsque vous voulez réinitialiser les composants du système, tels que les disques durs.

   - **Réduction de puissance.**

     Accélère l'UC.

     PRÉCAUTION : Si vous sélectionnez une action Platform Event shutdown (Arrêt suite à un événement de plateforme) autre que None (Aucun) ou Power Reduction (Réduction de puissance), votre système effectue un arrêt forcé lorsqu'un événement particulier survient. Cet arrêt est initialisé par le micrologiciel et est effectué sans arrêter le système d'exploitation en premier ou toute application en cours.

     REMARQUE : L'action Power reduction n'est pas prise en charge par tous les systèmes. Les fonctions Power Supply Monitoring (Surveillance des blocs d'alimentation) et Power Monitoring (Surveillance de l'alimentation) sont disponibles uniquement sur les systèmes sur lesquels sont installés au moins deux blocs d'alimentation redondants remplaçables à chaud. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondants installés de manière permanente qui ne disposent pas de circuits de gestion de l'alimentation.

6. Sélectionnez la case à cocher **Generate Alert** (Génération d'une alerte) pour les alertes à envoyer.

   REMARQUE : Pour générer une alerte, vous devez à la fois sélectionner les paramètres **Generate Alert** (Générer une alerte) et **Enable Platform Events Alerts** (Activer les alertes d'événements de plateforme).

7. Cliquez sur **Appliquer**.
8. Cliquez sur **Apply to Platform Events Page** (Appliquer à la page Événements sur plateforme) pour revenir à la fenêtre **Filtres d'événements sur plateforme**.

Définition des destinations des alertes d'événements de plateforme

Vous pouvez également utiliser la fenêtre Platform Event Filters (Filtres d'événement de plate-forme) pour sélectionner la destination d'une alerte d'événement de plate-forme. Selon le nombre de destinations affichées sur le système, vous pouvez définir une adresse IP distincte pour chaque adresse de destination. Une alerte d'événement de plate-forme est envoyée à chaque adresse IP de destination que vous définissez.

1. Cliquez sur **Configure Destinations** (Configurer les destinations) dans la fenêtre Platform Event Filters.
2. Cliquez sur le numéro de la destination que vous voulez configurer.

   REMARQUE : Le nombre de destinations que vous pouvez configurer sur un système varie.
3. Cochez la case **Activer la destination**.
4. Cliquez sur le **Destination Number** (Numéro de destination) pour saisir une adresse IP individuelle pour cette destination. Cette adresse IP est l'adresse IP à laquelle l'alerte d'événement de plate-forme est envoyé.

   REMARQUE : Sur les systèmes 12G dotés de versions spécifiques iDRAC7, vous pouvez définir la destination des événements de plateforme en tant que IPv4, IPv6 ou FQDN.
5. Entrez une valeur dans le champ **Chaîne de communauté** devant faire office de mot de passe pour authentifier les messages envoyés entre la station de gestion et un système géré. La chaîne de communauté (appelée également nom de communauté) est envoyée dans chaque paquet entre la station de gestion et le système géré.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **Go Back to Platform Events Page** (Retour à la page Événements sur plateforme) pour revenir à la fenêtre **Platform Event Filters**.

6

Journaux de Server Administrator

Server Administrator vous permet d'afficher et de gérer les journaux du matériel, des alertes et des commandes. Tous les utilisateurs peuvent accéder aux journaux et imprimer les rapports depuis la page d'accueil de Server Administrator ou depuis son interface de ligne de commande. Les utilisateurs doivent être connectés avec des privilèges d'administrateur pour effacer les journaux, et doivent être connectés avec des privilèges d'administrateur ou d'utilisateur privilégié pour envoyer les journaux par email à leur contact de service désigné.

Pour en savoir plus sur l'affichage des journaux et sur la création de rapports depuis la ligne de commande, voir le *Dell OpenManage Server Administrator Command Line Interface User's Guide* (Guide d'utilisateur de l'interface de ligne de commande de Dell OpenManage Server Administrator) à l'adresse **dell.com/support/manuals**.

Lorsque vous consultez les journaux de Server Administrator, vous pouvez cliquer sur **Help** (Aide) () pour en savoir plus sur la fenêtre spécifique actuellement ouverte. L'aide du journal Server Administrator est disponible pour toutes les fenêtres auxquelles l'utilisateur a accès en fonction du niveau de privilège de l'utilisateur et des groupes de matériel et de logiciel que Server Administrator découvre sur le système géré.

Fonctionnalités intégrées

Cliquez sur un en-tête de colonne pour trier la colonne ou modifier le sens de tri de la colonne. En outre, chaque fenêtre du journal contient plusieurs boutons de tâches pouvant être utilisés pour gérer et prendre en charge votre système.

Boutons de tâche des fenêtres des journaux

Le tableau suivant répertorie les boutons de tâche des fenêtres des journaux.

Tableau 11. Boutons de tâche des fenêtres des journaux

Name (Nom)	Description
Imprimer	Pour imprimer une copie du journal sur votre imprimante par défaut .
Exporter	Pour enregistrer un fichier texte contenant les données du journal (avec les valeurs des différents champs de données séparées par un délimiteur personnalisable) à un emplacement que vous spécifiez.
E-mail	Pour créer un message électronique comprenant le contenu du journal en pièce jointe.
Effacer le journal	Pour effacer tous les événements du journal.
Enregistrer sous	Pour enregistrer le contenu du journal dans un fichier **.zip** .
Actualiser	Pour charger de nouveau le contenu du journal dans la zone de données de la fenêtre d'action.

REMARQUE : Pour en savoir plus sur l'utilisation des boutons de tâche, voir Task Buttons (Boutons de tâche).

Journaux de Server Administrator

Server Administrator fournit les journaux suivants :

- Journal du matériel
- Journal des alertes
- Journal des commandes

Journal du matériel

Sur les systèmes Dell PowerEdge 9G et 11G, utilisez le journal du matériel pour rechercher les éventuels problèmes de composants matériels de votre système. Le voyant d'état du journal du matériel passe en condition Critique () lorsque le fichier atteint sa pleine capacité (100%). Il existe deux journaux de matériel disponibles, en fonction de votre système : le journal Embedded System Management (ESM - Gestion de système intégré) et le journal System Event Log (SEL - Journal des événements système). Les journaux ESM et SEL sont chacun composés d'un ensemble d'instructions intégrées pouvant envoyer des messages de condition du matériel au logiciel Systems Management (logiciel de gestion des systèmes). Chaque composant répertorié dans les journaux possède en voyant d'état en regard de son nom. Le tableau suivant répertorie les voyants d'état.

Tableau 12. Voyant d'état de journal du matériel

Condition	Description
Une coche verte ()	indique qu'un composant est intègre (normal).
Un triangle jaune contenant un point d'exclamation ()	indique que le composant a une condition d'avertissement (non critique) et qu'il doit être vérifié.
Un X rouge ()	indique qu'un composant a une condition critique/défaillant et qu'il nécessite une intervention immédiate.
Un point d'interrogation ()	indique que la condition d'intégrité d'un composant est inconnue.

Pour accéder au journal du matériel, cliquez sur **System** (Système), puis sur l'onglet **Logs** (Journaux) et sur **Hardware** (Matériel).

Les informations affichées dans les journaux ESM et SEL comprennent :

- Le niveau de gravité de l'événement
- La date et l'heure auxquelles l'événement s'est produit
- La description de l'événement

Maintenance du journal du matériel

L'icône du voyant d'état située en regard du nom du journal sur la page d'accueil de Server Administrator passe d'une condition normale () à une condition non critique () lorsque le fichier journal atteint une capacité de 80 pourcent. Assurez-vous que vous pouvez supprimer le journal du matériel lorsqu'il atteint une capacité de 80 pourcent. Si le journal atteint une capacité de 100 pourcent, les derniers événements sont supprimés du journal.

Pour effacer le journal du matériel, cliquez sur le lien **Clear Log** (Effacer le journal) de la page **Hardware Log** (Journal du matériel).

Journal des alertes

REMARQUE : Si le journal des alertes affiche des données XML non valides (par exemple, lorsque les données XML générées pour la sélection ne sont pas bien formées), cliquez sur **Clear Log** (Effacer le journal), puis affichez à nouveau les informations du journal.

Utilisez le journal des alertes pour surveiller les divers éléments système. Server Administrator génère les événements en réponse aux modifications de la condition des capteurs et autres paramètres surveillés. Chaque événement de modification de condition enregistré dans le journal des alertes consiste en un identifiant unique appelé ID d'événement, correspondant à une catégorie source d'événements, et d'un message d'événement qui décrit l'événement en question. L'ID d'événement et le message décrivent de manière unique la gravité et la cause de l'événement et fournissent d'autres informations pertinentes, telles que l'emplacement de l'événement et la condition précédente du composant surveillé.

Pour accéder au journal des alertes, cliquez sur **System** (Système), puis sur l'onglet **Logs** (Journaux) et sur **Alert** (Alerte).

Les informations affichées dans le Journal des alertes comprennent :

- Le niveau de gravité de l'événement
- L'ID de l'événement
- La date et l'heure auxquelles l'événement s'est produit
- La catégorie de l'événement
- La description de l'événement

REMARQUE : L'historique du journal peut être requis en cas de dépannages et diagnostics futurs. Par conséquent, il est recommandé d'enregistrer les fichiers journaux.

Pour des informations détaillées sur les messages d'alertes, voir le *Server Administrator Messages Reference Guide* (Guide de référence des messages de Server Administrator) à l'adresse **dell.com/support/manuals**.

Journal des commandes

REMARQUE : Si le journal des commandes affiche des données XML non valides (par exemple, lorsque les données XML générées pour la sélection ne sont pas bien formées), cliquez sur **Clear Log** (Effacer le journal), puis affichez à nouveau les informations du journal.

Utilisez le journal des commandes pour surveiller toutes les commandes émises par les utilisateurs Server Administrator. Le journal des commandes effectue le suivi des ouvertures de session, fermetures de session, initialisations du logiciel Systems Management et arrêts initialisés par le logiciel Systems Management, et enregistre le dernier effacement du journal. La taille du fichier du journal des commandes peut être spécifiée, sur demande.

Pour accéder au journal de commandes, cliquez sur **System** (Système), puis sur l'onglet **Logs** (Journaux) et enfin sur **Command** (Commande).

Les informations affichées dans le journal des commandes comprennent :

- La date et l'heure auxquelles la commande a été invoquée
- L'utilisateur actuellement connecté à la page d'accueil de Server Administrator ou à la CLI
- Une description de la commande et des valeurs qui lui sont associées

REMARQUE : L'historique du journal peut être requis en cas de dépannages et diagnostics futurs. Par conséquent, il est recommandé d'enregistrer les fichiers journaux.

7

Définition d'actions d'alerte

Définition d'actions d'alerte pour les systèmes exécutant des systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge

Lorsque vous définissez les actions d'alerte pour un événement, vous pouvez spécifier l'action pour afficher une alerte sur le serveur. Pour effectuer cette action, Server Administrator envoie un message à **/dev/console**. Si le système Server Administrator exécute un X Window System, le message ne s'affiche pas. Pour afficher le message d'alerte sur un système Red Hat Enterprise Linux lorsque le X Window System est en cours d'exécution, vous devez démarrer **xconsole** ou **xterm -C** avant que l'événement ne se produise. Pour voir le message d'alerte sur un système SUSE Linux Enterprise Server alors que le X Window System est en cours d'exécution, vous devez démarrer un terminal tel que **xterm -C** avant que l'événement ne se produise.

Lorsque vous définissez des actions d'alerte pour un événement, vous pouvez spécifier l'action pour **Diffuser un message**. Pour ce faire, Server Administrator exécute la commande wall qui envoie le message aux personnes connectées dont l'autorisation de message est définie sur **oui**. Si le système exécutant Server Administrator exécute un X Window System, le message ne s'affiche pas par défaut. Pour afficher le message de diffusion lorsque X Window System est actif, vous devez démarrer un terminal, tel que **xterm** ou **gnome-terminal**, avant que l'événement ne se produise.

Lorsque vous définissez les actions d'alerte pour un événement, vous pouvez spécifier l'action pour **exécuter l'application**. Les applications que Server Administrator peut exécuter ont des limites. Pour assurer une exécution correcte :

- Ne spécifiez pas d'applications basées sur X Window System, car Server Administrator ne peut pas exécuter ces applications correctement.
- Ne spécifiez pas d'applications qui requièrent une entrée de la part de l'utilisateur, car Server Administrator ne peut pas exécuter ces applications correctement.
- Redirigez **stdout** et **stderr** vers un fichier lorsque vous spécifiez l'application pour pouvoir voir les résultats ou les messages d'erreur.
- Si vous voulez exécuter plusieurs applications (ou commandes) pour une alerte, créez un script à cet effet et indiquez le chemin complet du script dans la case **Absolute path to the application box** (Chemin absolu de l'application).

Exemple 1 : `ps -ef >/tmp/psout.txt 2>&1`

La commande de l'exemple 1 exécute l'application ps et redirige stdout et **stderr** vers le fichier **/tmp/psout.txt**.

Exemple 2 : `mail -s "Server Alert" admin </tmp/alertmsg.txt>/tmp/mailout.txt 2>&1`

La commande de l'exemple 2 exécute l'application de courrier et envoie le message du fichier **/tmp/alertmsg.txt** à l'utilisateur Red Hat Enterprise Linux ou SUSE Linux Enterprise Server et à l'administrateur, avec comme objet **Server Alert** (Alerte du serveur). Le fichier **/tmp/alertmsg.txt** doit être créé par l'utilisateur avant que cet événement ne se produise. En outre, **stdout** et **stderr** sont redirigés vers le fichier **/tmp/mailout.txt** au cas où une erreur survienne.

Définition des actions d'alerte sous Microsoft Windows Server 2003 et Windows Server 2008

Lors de la spécification d'actions d'alerte, les scripts Visual Basic ne sont pas automatiquement interprétés par la fonction Execute Application (Exécuter l'application), bien que vous puissiez exécuter un fichier `.cmd, .com, .bat` ou `.exe` en spécifiant uniquement le fichier comme action d'alerte.

Pour résoudre ce problème, appelez d'abord le processeur de commande `cmd.exe` pour démarrer le script. Par exemple, l'action d'alerte pour exécuter une application peut être définie comme suit :

```
c:\winnt\system32\cmd.exe /c d:\example\example1.vbs
```

où `d:\example\example1.vbs` est le chemin complet vers le fichier de script.

Ne définissez pas un chemin vers une application interactive (une application disposant d'une interface utilisateur graphique ou qui nécessite l'entrée de données par l'utilisateur) dans le champ Absolute Path to the Application (Chemin absolu de l'application). L'application interactive peut ne pas fonctionner normalement sur certains systèmes d'exploitation.

REMARQUE : Vous devez spécifier le chemin complet pour les fichiers **cmd.exe** et script.

REMARQUE : Microsoft Windows 2003 n'est pas pris en charge sur les systèmes 12G.

Définition de l'action d'alerte Exécuter l'application sous Windows Server 2008

Pour des raisons de sécurité, Windows Server 2008 est configuré pour ne pas autoriser les services interactifs. Lorsqu'un service est installé comme service interactif sur Windows Server 2008, le système d'exploitation consigne un message d'erreur dans le journal du système Windows sur le service à marquer comme service interactif.

Lorsque vous utilisez Server Administrator pour configurer des actions d'alerte pour un événement, vous pouvez définir l'action pour « exécuter une application ». Pour pouvoir exécuter des applications interactives correctement pour une action d'alerte, vous devez configurer le service de gestion des données DSM SA (Dell Systems Management Server Administrator) comme service interactif. Les applications dotées d'une interface utilisateur graphique ou qui demandent à l'utilisateur d'entrer des données, telles que la commande pause dans un fichier séquentiel, sont des exemples d'applications interactives.

Lorsque Server Administrator est installé sur Microsoft Windows Server 2008, le service DSM SA Data Manager est installé comme service non interactif, ce qui implique qu'il est configuré pour ne pas interagir avec le bureau par défaut. Par conséquent, les applications interactives ne s'exécutent pas correctement lorsqu'elles sont exécutées pour une action d'alerte. Si une application interactive est exécutée pour une action d'alerte dans ce cas, l'application est suspendue et attend l'entrée de données. L'interface d'application/invite n'est pas visible et reste invisible, même après le démarrage du service de détection de services interactifs. L'onglet **Processes** (Processus) dans le gestionnaire des tâches affiche une entrée d'avancement d'application pour chaque exécution de l'application interactive.

Si vous avez besoin d'exécuter une application interactive pour une action d'alerte sur Microsoft Windows Server 2008, vous devez configurer le service DSM SA Data Manager pour être autorisé à interagir avec le bureau.

Pour autoriser l'interaction avec le bureau :

- Effectuez un clic droit sur le service Gestionnaire de données DSM SA dans le volet **Services control** (Contrôle des services), puis sélectionnez **Properties** (Propriétés).
- Dans l'onglet **Log On** (Ouvrir une session), sélectionnez **Allow service to interact with desktop** (Autoriser le service à interagir avec le Bureau) et cliquez sur **OK**.
- Redémarrez le service DSM SA Data Manager pour appliquer les modifications.

- Assurez-vous que le service **Interactive Services Detection** (Détection des services interactifs) est en cours d'exécution.

Lorsque vous redémarrez le service DSM SA Data Manager avec ce changement, le Service Control Manager (Gestionnaire de contrôle de service) journalise le message suivant sur le journal du système :

```
Le service DSM SA Data Manager est marqué comme service interactif. L'activation
du service Interactive Services Detection permet au service DSM SA Data Manager
d'exécuter correctement les applications interactives pour une action d'alerte.
```

Une fois ces changements effectués, la boîte de dialogue **Interactive services dialog detection** (Détection de boîte de dialogue de services interactifs) est affichée par le système d'exploitation, offrant l'accès à l'interface/l'invite de l'application interactive.

Messages d'alertes de filtres d'événements sur plateforme du contrôleur BMC/iDRAC

Le tableau qui suit répertorie tous les messages PEF (Platform Event Filter) (filtre d'événement sur plateforme) possibles ainsi qu'une description pour chaque événement.

Tableau 13. Événements d'alerte PEF

Événement	Description
Échec signalé par le capteur de ventilateur	Le ventilateur fonctionne trop lentement ou il est arrêté.
Échec signalé par le capteur de tensions	La tension est trop basse pour un fonctionnement correct.
Avertissement du capteur de batterie	La batterie fonctionne en dessous du niveau recommandé de charge.
Échec signalé par le capteur de batterie	La batterie est défaillante.
Échec signalé par le capteur discret de ventilateur	La tension est trop basse pour un fonctionnement correct.
Avertissement du capteur de température	La température devient trop élevée ou trop basse.
Échec signalé par le capteur de température	La température est trop élevée ou trop basse pour un fonctionnement normal.
Détection d'une intrusion dans le châssis	Le châssis du système a été ouvert
Redondance (bloc d'alimentation ou ventilateur) dégradée	La redondance des ventilateurs et/ou des blocs d'alimentation est réduite.
Redondance (bloc d'alimentation ou ventilateur) perdue	Aucune redondance pour les ventilateurs et/ou les blocs d'alimentation du système.
Avertissement de processeur	Les performances ou la vitesse d'un processeur ne sont pas maximales.
Échec du processeur	Un processeur est défaillant.
Processeur absent	Le processeur a été retiré.
Avertissement concernant PS/VRM/D2D	Le bloc d'alimentation, le module régulateur de tension ou le convertisseur CC-CC est sur le point d'être défaillant.
Panne de PS/VRM/D2D	Le bloc d'alimentation, le module régulateur de tension ou le convertisseur CC-CC est défaillant.

Événement	Description
Journal du matériel plein ou vide	Un journal de matériel vide ou saturé nécessite l'intervention de l'administrateur.
Récupération automatique du système	Le système est bloqué ou ne répond pas et exécute l'action définie par la récupération automatique du système.
Avertissement du capteur d'alimentation du système	La consommation d'énergie est proche du seuil de défaillance.
Échec signalé par le capteur de puissance système	La consommation électrique a dépassé la limite maximale acceptable et a généré un échec.
Média flash amovible absent	Le média flash amovible a été retiré.
Échec du média flash amovible	Le média flash amovible est sur le point d'être défaillant.
Avertissement du média flash amovible	Le média flash amovible est sur le point d'être défaillant.
Carte du module SD double interne critique	La carte du module SD double interne est défaillante.
Avertissement de la carte du module SD double interne	La carte du module SD double interne est sur le point d'être défaillante.
Redondance perdue pour la carte du module SD double interne	La carte du module SD double interne n'a pas de redondance.
Carte du module SD double interne absente	La carte du module SD double interne a été retirée.

8

Dépannage

Échec du service de connexion

Sur Red Hat Enterprise Linux, lorsque SELinux est défini sur le mode `enforced` (forcé), le service Dell Systems Management Server Administrator (SM SA) Connection ne parvient pas à démarrer. Réalisez une des étapes suivantes et démarrez ce service :

- Définissez `SELinux` sur le mode Disabled (Désactivé) ou sur le mode Permissive (Permissif).
- Modifiez la propriété **allow_execstack** SELinux et faites-la passer à l'état **ON** (Activé). Exécutez la commande suivante :

  a. `setsebool allow_execstack on`
- Modifiez le contexte de sécurité du service SM SA connection service. Exécutez la commande suivante :

`chcon -t unconfined_execmem_t`

/opt/dell/srvadmin/sbin/dsm_om_connsvcd

Scénarios d'échec d'ouverture de session

Il se peut que vous ne puissiez pas ouvrir une session sur le système géré si :

- vous entrez une adresse IP non valide/incorrecte.
- vous entrez des informations d'identification incorrectes (nom d'utilisateur et mot de passe).
- le système géré est ÉTEINT.
- le système géré n'est pas accessible en raison d'une erreur de DNS ou d'adresse IP non valide.
- le système géré détient un certificat non approuvé et vous ne sélectionnez pas **Ignore Certificate Warning** (Ignorer l'avertissement de certificat) sur la page d'ouverture de session
- Les services de Server Administrator ne sont pas activés sur le système VMware ESX/ESXi. Pour en savoir plus sur l'activation des services Server Administrator sur le système VMware ESX/ESXi, consultez le *Dell OpenManage Server Administrator Installation Guide* (Guide d'installation de Dell OpenManage Server Administrator) à l'adresse **dell.com/support/manuals**.
- Le service SFCBD (small footprint CIM broker daemon) du système VMware ESX/ESXi ne s'exécute pas.
- Le service Web Server Management Service du système géré ne s'exécute pas.
- Vous entrez l'adresse IP du système géré et non le nom d'hôte lorsque vous ne cochez pas la case **Ignore Certificate Warning** (Ignorer l'avertissement de certificat).
- La fonction WinRM Authorization (Autorisation WinRM) (Remote Enablement - Activation à distance) n'est pas configuré dans le système géré. Pour en savoir plus sur cette fonction, consultez le *Dell OpenManage Server Administrator Installation Guide* (Guide d'installation de Dell OpenManage Server Administrator) disponible à l'adresse **dell.com/support/manuals**.
- Un échec d'authentification se produit lors de la connexion à un système d'exploitation VMware ESXi 4.1/ESX 5.0, pouvant être dû à l'une des raisons suivantes :

  a. Le mode `lockdown` est activé lorsque vous vous connectez au serveur ou lorsque vous vous connectez à Server Administrator. Voir la documentation VMware pour en savoir plus sur le mode `lockdown`.

b. Le mot de passe a été modifié alors que votre session Server Administrator est active.

c. Vous vous connectez à Server Administrator en tant qu'utilisateur normal sans privilèges d'administrateur. Pour en savoir plus, voir la documentation VMware sur l'attribution du rôle.

Correction d'une installation défaillante de Server Administrator sur un système d'exploitation Windows pris en charge

Vous pouvez réparer une installation défectueuse en forçant une réinstallation et en effectuant ensuite une désinstallation de Server Administrator.

Pour forcer une réinstallation :

1. Vérifiez la version de Server Administrator installée précédemment.
2. Depuis le site **support.dell.com**, téléchargez le progiciel d'installation correspondant à cette version.
3. Localisez **SysMgmt.msi** dans le répertoire **srvadmin\windows\SystemsManagement**.
4. Pour effectuer une réinstallation forcée, tapez la commande suivante à l'invite de commande
   `msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vamus`
5. Sélectionnez **Custom Setup** (Installation personnalisée) et choisissez toutes les fonctionnalités installées à l'origine. Si vous n'êtes pas certain des éléments initialement installés, sélectionnez-les tous et lancez l'installation.

   REMARQUE : Si vous avez installé Server Administrator dans un répertoire autre que celui par défaut, veillez à effectuer également la modification dans **Custom Setup**.

   REMARQUE : Lorsque l'application est installée, vous pouvez désinstaller Server Administrator via **Add/ Remove Programs** (Ajout/Suppression de programmes).

Services OpenManage Server Administrator

Ce tableau répertorie les services utilisés par Server Administrator pour fournir des informations sur la gestion de systèmes et les conséquences engendrées par la panne de ces services.

Tableau 14. Services OpenManage Server Administrator

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
Windows : SM SA Connection Service Linux : `dsm_om_connsvc` (Ce service est installé avec Server Administrator Web Server.)	Fournit un accès à distance/local à Server Administrator à partir de n'importe quel système doté d'un navigateur Web pris en charge et d'une connexion réseau.	Les utilisateurs ne sont pas capables de se connecter à Server Administrator et de réaliser des opérations via l'interface utilisateur Web. Cependant, la CLI peut encore utilisée.	Redémarrer le service	Critique
Windows : SM SA Shared Services Linux: `dsm_om_shrsvc` (Ce service s'exécute sur le système géré.)	Exécute le collecteur d'inventaire au démarrage pour effectuer un inventaire des logiciels du système. Celui-ci permet aux	Les mises à jour des logiciels ne sont réalisables qu'à l'aide d'ITA. Cependant, les mises à jour peuvent être effectuées localement et à	Redémarrer le service	Avertissement

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
	fournisseurs SNMP et CIM de Server Administrator d'effectuer une mise à jour des logiciels à distance à l'aide de Dell System Management Console et Dell IT Assistant (ITA).	l'extérieur de Server Administrator à l'aide de DUP individuels. Les mises à jour peuvent encore être réalisées à l'aide d'outils tiers (par exemple, MSSMS, Altiris et Novell ZENworks).		

REMARQUE : Si les bibliothèques de compatibilité 32 bits ne sont pas installées sur un système Linux 64 bits, les services partagés ne parviennent pas à démarrer le collecteur de l'inventaire et affiche le message d'erreur suivant : `libstdc++.so.5 is required to run the Inventory Collector` (la bibliothèque libstdc++.so.5 est requise pour exécuter le collecteur de l'inventaire). La commande **srvadmin-cm.rpm** fournit les valeurs binaires du collecteur de l'inventaire. Pour consulter la liste des RPM dont srvadmin-cm dépend, voir le *OpenManage Server Administrator Installation Guide* (Guide d'installation d'OpenManage Server Administrator) disponible sur **dell.com/support/manuals**.

REMARQUE : Le collecteur d'inventaire est requis pour mettre à jour les consoles Dell à l'aide des progiciels de mise à jour Dell (DUP).

REMARQUE : Certaines fonctionnalités du collecteur d'inventaire ne sont pas prises en charge par (64 bits).

Windows : SM SA Data Manager Linux : `dsm_sa_datamgrd` (hébergé sous le service dataeng) (Ce service s'exécute sur le système géré.)	Surveille le système, fournit un accès rapide à des informations détaillées sur les pannes et les performances, et permet l'administration à distance de systèmes surveillés, y compris l'arrêt, le démarrage et la sécurité.	Les utilisateurs ne peuvent pas configurer/afficher des détails sur le niveau matériel depuis l'interface GUI/CLI si ces services ne sont pas en cours d'exécution.	Redémarrer le service	Critique
Windows : SM SA Data Manager Linux : `dsm_sa_eventmgrd` (hébergé sous le service dataeng) (Ce service s'exécute sur le système géré.)	Fournit un service de journalisation des événements en rapport au système d'exploitation et aux fichiers en vue de la gestion de systèmes. Il est également utilisé par les analyseurs de journaux d'événements.	Si ce service est arrêté, les fonctions de journalisation des événements ne fonctionnent pas correctement.	Redémarrer le service	Avertissement
Linux : `dsm_sa_snmpd` (hébergé sous le service dataeng) (Ce	Interface Data Engine Linux SNMP	Les demandes SNMP get/set/trap ne fonctionnent pas à	Redémarrer le service	Critique

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
service s'exécute sur le système géré.)		partir d'une station de gestion.		
Windows : `mr2kserv` (Ce service s'exécute sur le système géré.)	Le service Storage Management fournit des informations sur la gestion du stockage et des fonctionnalités avancées pour configurer un stockage local ou distant rattaché à un système.	Les utilisateurs ne peuvent pas exécuter de fonctions de stockage pour tous les contrôleurs RAID et non RAID pris en charge.	Redémarrer le service	Critique

9

Questions fréquemment posées

Cette section répertorie les questions les plus fréquentes concernant OpenManage Server Administrator.

REMARQUE : Ces questions ne sont pas spécifiques à cette version de Server Administrator.

1. **Pourquoi les fonctionnalités de redémarrage des hôtes ESXi 4.x (4.0 U3) et ESXi 5.x échouent-elles depuis OpenManage Server Administrator ?**

   Ce problème découle de la clé de licence SAL (stand alone license - licence autonome) VMware. Pour en savoir plus, consultez l'article connexe de la base de connaissances sur **kb.vmware.com/kb/kb1026060**.

2. **Quelles sont les tâches à exécuter après l'ajout d'un système d'exploitation VMware ESX 4.0 U3 ou ESX 4.1 U2 à un domaine Active Directory ?**

   Après avoir ajouté un système d'exploitation VMware ESX 4.0 U3 and ESX 4.1 U2 à un domaine Active Directory, un utilisateur Active Directory doit procéder comme suit :

   a. Se connecter à Server Administrator depuis le système exécutant le système d'exploitation VMware ESX 4.0 U3 et ESX 4.1 U2 et redémarrer le service de connexion DSM SA.

   b. Se connecter au nœud distant en utilisant le système d'exploitation VMware ESX 4.0 U3 et ESX 4.1 U2 en tant qu'agent d'activation à distance. Patientez environ 5 minutes pendant que le processus sfcbd ajoute la permission au nouvel utilisateur.

3. **Quel est le niveau de permission minimum requis pour installer Server Administrator ?**

   Pour installer Server Administrator, vous devez disposer de privilèges d'administrateur. Les utilisateurs et utilisateurs privilégiés ne sont pas autorisés à installer Server Administrator.

4. **Existe-t-il un chemin de mise à niveau requis pour installer Server Administrator ?**

   Pour les systèmes exécutant Server Administrator 4.3, vous devez effectuer une mise à niveau à une version 6.*x* puis à la version 7.*x*. Pour les systèmes exécutant une version antérieure à 4.3, vous devez effectuer une mise à niveau à la version 4.3, puis à une version 6.*x* et enfin à la version 7.*x* (*x* indique la version de Server Administrator vers laquelle vous souhaitez vous mettre à niveau).

5. **Comment puis-je déterminer la dernière version de Server Administrator disponible pour mon système ?**

   Connectez-vous à **support.dell.com** → Enterprise IT → Manuals → Software → Systems Management → OpenManage Server Administrator (Enterprise IT > Manuels > Logiciels > Gestion des systèmes > OpenManage Server Administrator).

   La dernière version de la documentation reflète la version d'OpenManage Server Administrator à laquelle vous pouvez accéder.

6. **Comment puis-je savoir quelle version de Server Administrator s'exécute sur mon système ?**

   Une fois que vous êtes connecté à Server Administrator, naviguez vers **Properties** → **Summary** (Propriétés → Résumé). Vous trouverez la version de Server Administrator installée sur votre système dans la colonne **Systems Management** (Gestion des systèmes).

7. **Existe-t-il d'autres ports que les utilisateurs peuvent employer à part le port 1311 ?**

   Oui, vous pouvez définir le port https que vous souhaitez. Naviguez vers **Preferences** → **General Settings** → **Web Server** →**HTTPS Port** (Préférences > Paramètres généraux > Serveur Web > Port HTTPS)

   Au lieu de cliquer sur **Use default** (Utiliser la valeur par défaut), cliquez sur **Use Radio Button** (Utiliser le bouton radio) pour définir votre port préféré.

REMARQUE : Si le nouveau numéro de port est un numéro non valide ou utilisé, cela peut empêcher d'autres applications ou navigateurs d'accéder à Server Administrator sur le système géré. Pour consulter la liste des ports par défaut, voir le *Dell OpenManage Installation and Security User's Guide* (Guide d'utilisation concernant l'installation et la sécurité Dell OpenManage) sur **dell.com/support/manuals**.

8. **Puis-je installer Server Administrator sur Fedora, College Linux, Mint, Ubuntu, Sabayon ou PClinux ?**

   Non, Server Administrator ne prend pas en charge ces systèmes d'exploitation.

9. **Est-ce que Server Administrator peut envoyer des e-mails en cas de problème ?**

   Non, Server Administrator n'est pas conçu pour envoyer des e-mails en cas de problème.

10. **Le protocole SNMP est-il requis pour la découverte ITA, l'inventaire et les mises à jour logicielles sur des systèmes PowerEdge ? Le protocole CIM peut-il être utilisé seul pour la découverte, l'inventaire et les mises à jour ou SNMP est-il requis ?**

    Communication ITA *avec les systèmes Linux* :

    Le protocole SNMP est requis sur les systèmes Linux pour la découverte, l'obtention de la condition et l'inventaire.

    Les mises à jour de logiciel Dell s'effectuent via une session SSH et un FTP sécurisé ; en outre, des permissions/références de niveau root (racine) sont requises pour cette action discrète et exigées lorsque l'action est configurée ou demandée. Les références de la plage de découverte ne sont pas présumées.

    Communication ITA avec les systèmes Windows :

    Pour les serveurs (systèmes exécutant les systèmes d'exploitation Windows Server), le système peut être configuré avec le protocole SNMP et/ou CIM en vue de la découverte par ITA. L'inventaire nécessite le protocole CIM.

    Les mises à jour de logiciel, comme sous Linux, ne sont pas liées à la découverte et à l'interrogation, ni aux protocoles utilisés.

    À l'aide des références de niveau administrateur exigées au moment de la planification ou de l'exécution d'une mise à jour, un partage d'administration (lecteur) est établi sur un lecteur du système cible, et une copie de fichier(s) d'un endroit quelconque (éventuellement un autre partage réseau) est effectuée sur le système cible. Les fonctions WMI sont alors appelées pour exécuter la mise à jour de logiciel.

    Pour les clients/stations de travail, Server Administrator n'est pas installé ; par conséquent, la découverte CIM est utilisée lorsque la cible exécute OpenManage Client Instrumentation.

    Pour de nombreux autres périphériques comme les imprimantes réseau, le protocole SNMP constitue toujours la norme pour communiquer avec (essentiellement découvrir) le périphérique.

    Certains périphériques, tels que le périphérique de stockage EMC, possèdent des protocoles propriétaires. Certaines informations concernant cet environnement peuvent être obtenues en consultant les tableaux des ports utilisés figurant dans la documentation OpenManage.

11. **Existe-t-il des plans pour la prise en charge de SNMP v3 ?**

    Non, aucune prise en charge de SNMP v3 n'est prévue.

12. **Un caractère de trait de soulignement dans le nom de domaine peut-il provoquer des problèmes d'ouverture de session d'administrateur du serveur ?**

    Oui, un caractère de trait de soulignement dans le nom de domaine est non valide. Tous les autres caractères spéciaux (à part le tiret) sont également non valides. Utilisez uniquement des lettres sensibles à la casse et des chiffres.

13. **Quel est l'impact de la sélection/désélection d'« Active Directory » sur la page d'ouverture de session de Server Administrator sur les niveaux de privilège ?**

    Si vous ne cochez pas la case Active Directory, vous n'aurez accès qu'aux éléments configurés dans Microsoft Active Directory. Vous ne pourrez pas non plus vous connecter avec la solution de schéma étendu dans Microsoft Active Directory.

Cette solution vous permet de donner l'accès à Server Administrator, ce qui signifie qu'elle vous permet d'ajouter/contrôler les utilisateurs Server Administrator et les privilèges des utilisateurs existants dans votre logiciel Active Directory. Pour en savoir plus, voir « Using Microsoft Active Directory » (Utilisation de Microsoft Active Directory) dans le *Dell OpenManage Server Administrator Installation Guide* (Guide d'installation de Dell OpenManage Server Administrator) disponible à l'adresse **dell.com/support/manuals**.

14. **Quelles actions dois-je entreprendre lorsque je réalise une authentification Kerberos et tente de me connecter à partir de Web Server ?**

    Pour l'authentification, le contenu des fichiers **/etc/pam.d/openwsman** et **/etc/pam.d/sfcb**, sur le nœud géré, doit être remplacé par :

    Pour 32 bits :

    ```
    auth required pam_stack.so service=system-auth auth required /lib/security/
    pam_nologin.so account required pam_stack.so service=system-auth
    ```

    Pour 64 bits :

    ```
    auth required pam_stack.so service=system-auth auth required /lib64/
    security/pam_nologin.so account required pam_stack.so service=system-auth
    ```