

Dell EMC OpenManage Server Administrator
version 9.0.1
Guide d'utilisation

Remarques, précautions et avertissements

-  **REMARQUE** : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.
-  **PRÉCAUTION** : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.
-  **AVERTISSEMENT** : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Copyright © 2017 Dell Inc. ou ses filiales. Tous droits réservés. Dell, EMC et d'autres marques de commerce sont des marques de commerce de Dell Inc. ou de ses filiales. Les autres marques de commerce peuvent être des marques de commerce déposées par leurs propriétaires respectifs.

2017 - 06

Rév. A00

Table des matières

1 Introduction.....	6
Installation.....	6
Mise à jour de composants système particuliers.....	6
Storage Management Service.....	6
Instrumentation Service.....	7
Remote Access Controller.....	7
Journaux	7
What is new in this release.....	7
Disponibilité des normes de gestion des systèmes.....	7
Availability on supported operating systems.....	8
Page d'accueil de Server Administrator.....	8
Autres documents utiles.....	8
Accès aux documents à partir du site de support.....	10
Obtention d'une assistance technique.....	10
Contacter Dell EMC.....	10
2 Configuration et administration.....	11
Contrôle des accès basé sur des rôles.....	11
Privilèges utilisateur.....	11
Authentification.....	12
Authentification de Microsoft Windows.....	12
Authentification de Red Hat Enterprise Linux et de SUSE Linux Enterprise Server.....	12
Authentification de VMware ESXi Server.....	12
Cryptage.....	12
Attribution des privilèges d'utilisateur.....	12
Ajout d'utilisateurs à un domaine sur les systèmes d'exploitation Windows.....	13
Création d'utilisateurs Server Administrator sur les systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge.....	13
Désactivation de comptes d'invités et anonymes sur des systèmes d'exploitation Windows pris en charge.....	15
Configuring The SNMP Agent.....	15
Configuration du pare-feu sur les systèmes exécutant les systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge.....	20
3 Using Server Administrator.....	22
Ouverture et fermeture de session.....	22
Ouverture d'une session Server Administrator sur le système local	22
Server Administrator Managed System Login — Using the Desktop Icon.....	22
Connexion au système géré de Server Administrator — Utilisation du navigateur Web.....	23
Ouverture d'une session Central Web Server.....	23
Utilisation de l'ouverture de session Active Directory.....	24
Connexion directe.....	24

Configuration des paramètres de sécurité sur des systèmes exécutant un système d'exploitation Microsoft	
Windows pris en charge.....	24
Page d'accueil de Server Administrator.....	25
Différences d'interface utilisateur de Server Administrator au sein des systèmes modulaires et non modulaires.....	27
Barre de navigation globale.....	28
Arborescence système.....	28
Fenêtre d'action.....	28
Zone de données.....	29
Utilisation de l'aide en ligne.....	30
Utilisation de la page d'accueil Préférences.....	30
Préférences du système géré.....	31
Préférences de Server Administrator Web Server.....	31
Service de connexion Systems Management Server Administration et configuration de la sécurité.....	31
X.509 Certificate Management.....	33
Onglets d'actions de Server Administrator Web Server.....	34
Upgrading web server.....	35
Utilisation de l'interface de ligne de commande de Server Administrator.....	35

4 Services Server Administrator.....36

Gestion de votre système.....	36
Gestion des objets de l'arborescence du système/module de serveur.....	36
Objets de l'arborescence du système de la page d'accueil de Server Administrator.....	37
Enceinte modulaire.....	37
Accès et utilisation de Chassis Management Controller.....	37
Propriétés du système/Module de serveur.....	38
Châssis de système principal/Système principal.....	40
Gestion des préférences : Options de configuration de la page d'accueil.....	50
General settings.....	50
Server Administrator.....	51

5 Working with remote access controller 52

Affichage des informations de base.....	53
Configuration du périphérique d'accès à distance pour utiliser une connexion LAN.....	54
Configuration du périphérique d'accès à distance pour utiliser une connexion par port série.....	55
Configuration du périphérique d'accès à distance pour utiliser une communication série sur le LAN.....	56
Configuration supplémentaire pour iDRAC.....	56
Configuration des utilisateurs du périphérique d'accès à distance.....	57
Setting Platform Event Filter Alerts.....	57
Définition des destinations des alertes d'événements de plateforme.....	58

6 Journaux de Server Administrator.....59

Fonctionnalités intégrées.....	59
Boutons de tâche des fenêtres des journaux.....	59
Journaux de Server Administrator.....	59
Journal du matériel.....	60
Journal des alertes	60

Journal des commandes	61
7 Définition d'actions d'alerte	62
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.....	62
Setting Alert actions in Windows Server to Execute Applications.....	62
Messages d'alertes de filtre d'événements sur plateforme du contrôleur BMC/iDRAC.....	63
8 Dépannage.....	65
Échec du service de connexion.....	65
Scénarios d'échec d'ouverture de session.....	65
Correction d'une installation défectueuse de Server Administrator sur un système d'exploitation Windows pris en charge.....	65
Services Server Administrator.....	66
9 Forum aux questions.....	68

Introduction


Server Administrator 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 modulaire. 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

You can install Server Administrator using the *Dell EMC Systems Management Tools and Documentation software*. The software provides a setup program to install, upgrade, and uninstall Server Administrator, managed system and management station software components. Also, you can install Server Administrator on multiple systems through an unattended installation across a network. The Server Administrator installer provides installation scripts and RPM packages to install and uninstall Server Administrator and other managed system software components on your managed system. For more information, see the *Dell EMC Server Administrator Installation Guide* and the *Management Station Software Installation Guide* at dell.com/opemanagementmanuals.

 **NOTE: When you install the open source packages from the *Dell EMC Systems Management Tools and Documentation software*, the corresponding license files are automatically copied to the system. When you remove these packages, the corresponding license files are also removed.**

 **NOTE: If you have a modular system, install Server Administrator on each server module installed in the chassis.**

Mise à jour de composants système particuliers

Pour mettre à jour des 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 mettre à jour un système dans son intégralité. L'utilitaire SUU (Server Update Utility) identifie les mises à jour requises et les applique 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 du système ou sur la consultation des mises à jour disponibles pour tout système répertorié dans le référentiel, voir le document *Dell Server Update Utility User's Guide* (Guide d'utilisation de l'utilitaire SUU) à l'adresse dell.com/openmanagementmanuals.**

Storage Management Service

The Storage Management Service provides storage management information in an integrated graphical view.

 **NOTE: For more information about the Storage Management Service, see the *Dell EMC Server Administrator Storage Management User's Guide* at dell.com/openmanagemanuals.**

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.

Remote Access Controller


The Remote Access Controller provides a complete remote system management solution for systems equipped with the Baseboard Management Controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) solution. The Remote Access Controller provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Controller also provides an alert notification when a system is down and allows you to remotely restart the system. Additionally, the Remote Access Controller logs the probable cause of system crashes and saves the most recent crash screen.

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.

What is new in this release

The release highlights of OpenManage Server Administrator are:

- Full Power Cycle.
- System Lockdown mode.
- NVDIMM Monitoring.
- Support for the following operating systems:
 - Support for Red Hat Enterprise Linux 6.9
 - VMware ESXi 6.5
 - VMware ESXi 6.0 U3
 -  **NOTE: Citrix XenServer operating system support has been dropped for Server Administrator and Storage Management.**
- Support for the following browsers:
 - Internet Explorer - 9, 10, 11
 - Microsoft Edge 25
 - Google Chrome - 58
 - Safari - 9.1
 - Mozilla Firefox - 52, 53

 **NOTE: For the list of supported operating systems and Dell servers, see the *Dell EMC OpenManage Software Support Matrix* in the required version of OpenManage Software at dell.com/openmanagemanuals.**

Disponibilité des normes de gestion des systèmes


Server Administrator prend en charge les protocoles de gestion de systèmes 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, installez et activez 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, parfois, de la version de celui-ci.

 **REMARQUE : Pour en savoir plus sur les problèmes de sécurité SNMP, consultez le fichier des notes de publication de Server Administrator (inclus avec l'application Server Administrator) ou rendez-vous sur dell.com/openmanagemanuals. Appliquez les mises à jour depuis les agents SNMP principaux de votre système d'exploitation pour vous assurer que les sous-agents SNMP sont sécurisés.**

Availability on supported operating systems

On supported Microsoft Windows operating systems, Server Administrator supports two systems management standards: CIM/Windows Management Instrumentation (WMI) and SNMP, while on supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator supports the SNMP systems management standard.

Server Administrator adds considerable security to these systems management standards. All attributes set operations (for example, changing the value of an asset tag) must be performed with Dell EMC OpenManage Essentials while logged in with the required privileges.

The following table shows the systems management standards that are available for each supported operating system.

Table 1. Systems Management Standards Availability

Operating system	SNMP	CIM
Windows Server 2012 R2 family	Available from the operating system installation media	Always installed
Red Hat Enterprise Linux	Available in the net-snmp package from the operating system installation media	Unavailable
SUSE Linux Enterprise Server	Available in the net-snmp package from the operating system installation media	Unavailable
VMware ESXi	SNMP trap support available	Available

 **NOTE: While ESXi supports SNMP traps, it does not support hardware inventory through SNMP.**

Page d'accueil de Server Administrator

La page d'accueil de **Server Administrator** permet d'exécuter des tâches de gestion système basées sur navigateur Web faciles à configurer et simples d'utilisation depuis le système géré ou depuis un hôte distant via un réseau local, un service d'accès commuté ou un réseau sans fil. Lorsque le service de connexion Systems Management Server Administration (DSM SA Connection Service) est installé et configuré sur le système géré, vous pouvez exécuter des fonctions de gestion à distance à partir de n'importe quel système doté d'un navigateur Web pris en charge et d'une connexion Internet. En outre, la page d'accueil de Server Administrator fournit une aide en ligne exhaustive et contextuelle.

Autres documents utiles

Outre ce guide, les manuels suivants sont disponibles sur dell.com/softwaresecuritymanuals.

- Le document *Dell EMC Systems Software Support Matrix* (Matrice de prise en charge logicielle des systèmes Dell EMC) fournit des informations sur les différents systèmes, les systèmes d'exploitation pris en charge par ces systèmes et les composants qui peuvent être installés sur ces systèmes.
- Le document *Dell EMC OpenManage Server Administrator Installation Guide* (Guide d'installation de Dell EMC OpenManage Server Administrator) contient les instructions d'installation de Dell EMC OpenManage Server Administrator.

- Le document *Dell EMC OpenManage Management Station Software Installation Guide* (Guide d'installation du logiciel de la station de gestion Dell EMC OpenManage Management) contient les instructions d'installation du logiciel de la station de gestion Dell EMC OpenManage.
- Le document *Dell EMC OpenManage SNMP Reference Guide* (Guide de référence de Dell EMC OpenManage SNMP) présente la base d'informations de gestion (MIB) du protocole simplifié de gestion de réseau (SNMP).
- Le document *Dell EMC OpenManage Server Administrator CIM Reference Guide* (Guide de référence CIM de Dell EMC OpenManage Server Administrator) présente le fournisseur du modèle commun d'informations (CIM) et un suffixe de fichier de format d'objet de gestion standard (MOF).
- Le document *Dell EMC Messages Reference Guide* (Guide de référence des messages Dell EMC) répertorie les messages qui s'affichent dans le journal des alertes de la page d'accueil de Server Administrator ou sur l'observateur d'événements de votre système d'exploitation.
- Le document *Dell EMC OpenManage Server Administrator Command Line Interface Guide* (Guide de l'interface de ligne de commande de Dell EMC OpenManage Server Administrator) présente l'interface de ligne de commande complète de Server Administrator.
- Le document *Dell Remote Access Controller User's Guide* (Guide d'utilisation de Dell Remote Access Controller) contient des informations exhaustives sur l'utilisation de l'utilitaire de ligne de commande RACADM pour configurer un DRAC.
- Le document *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.
- Le document *Command Line Reference Guide for iDRAC 6 and CMC* (Guide de référence de la ligne de commande pour iDRAC 6 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 document *Dell EMC OpenManage Server Administrator Storage Management User's Guide* (Guide d'utilisation de Dell EMC 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 document *Dell Remote Access Controller User's Guide* (Guide d'utilisation de Dell Remote Access Controller) fournit des informations complètes sur l'installation et la configuration d'un contrôleur DRAC, et sur son utilisation pour accéder à distance à un système qui ne fonctionne 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.
- Le document *Dell EMC OpenManage Server Update Utility User's Guide* (Guide d'utilisation de l'utilitaire Dell EMC OpenManage Server Update Utility) vous explique comment vous procurer et utiliser Server Update Utility (SUU) pour mettre à jour vos systèmes ou pour afficher les mises à jour disponibles pour n'importe quel système répertorié dans le référentiel.
- 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 document *Dell License Manager User's Guide* (Guide d'utilisation de Dell License Manager) fournit des informations sur la gestion des licences de serveur de composants pour les serveurs 12G.
- Le *Glossaire* offre des informations sur la terminologie utilisée dans le présent document.

Accès aux documents à partir du site de support

Vous pouvez accéder aux documents requis de l'une des façons suivantes :

- À l'aide des liens suivants :
 - Pour tous les documents Enterprise Systems Management (Gestion des systèmes Enterprise) : Dell.com/SoftwareSecurityManuals
 - Pour les documents OpenManage : Dell.com/OpenManageManuals
 - Pour les documents Remote Enterprise Systems Management (Gestion des systèmes Enterprise à distance) : Dell.com/esmanuals
 - Pour les documents iDRAC et Lifecycle Controller : Dell.com/idracmanuals
 - Pour les documents OpenManage Connections Enterprise Systems Management (Gestion des systèmes Enterprise - Connexions OpenManage) : Dell.com/OMConnectionsEnterpriseSystemsManagement
 - Pour les documents Serviceability Tools (Outils de facilité de la gestion) : Dell.com/ServiceabilityTools
 - Pour les documents Client Command Suite Systems Management : Dell.com/DellClientCommandSuiteManuals
- Sur le site de support :
 - a. Accédez à Dell.com/Support/Home.
 - b. Dans la section **Sélectionnez un produit**, cliquez sur **Logiciel et sécurité**.
 - c. Dans la zone de groupe **Software & Security (Logiciels et sécurité)**, cliquez sur le lien approprié parmi les liens suivants :
 - **Enterprise Systems Management (Gestion des systèmes Enterprise)**
 - **Remote Enterprise Systems Management (Gestion des systèmes Enterprise à distance)**
 - **Serviceability Tools (Outils de facilité de la gestion)**
 - **Dell Client Command Suite**
 - **Connections Client Systems Management (Gestion des systèmes Client - Connexions)**
 - d. Pour afficher un document, cliquez sur la version de produit requise.
- Avec les moteurs de recherche :
 - Saisissez le nom et la version du document dans la zone de recherche.

Obtention d'une assistance technique

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

En outre, une formation et une certification d'entreprise sont disponibles ; voir dell.com/training pour en savoir plus. Ce service n'est pas disponible partout.

Contacteur Dell EMC

 **REMARQUE : En l'absence de connexion Internet active, vous trouverez les informations de contact sur la preuve d'achat, le bon de livraison, la facture ou dans le catalogue de produits.**

Dell EMC propose plusieurs options de services et support en ligne et par téléphone. La disponibilité des services varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre zone géographique. Pour toute question commerciale, de support technique ou de service à la clientèle, n'hésitez pas à contacter Dell EMC :

Rendez-vous sur Dell.com/contactdell.

Configuration et administration

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 <i>utilisateurs</i> peuvent afficher la plupart des informations.
Utilisateur privilégié	Oui	Oui	Les <i>utilisateurs privilégiés</i> 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 <i>administrateurs</i> 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, ainsi que supprimer les journaux de matériel, d'événements et de commandes. Les administrateurs peuvent également configurer le système de sorte à envoyer des e-mails.
Administrateur élevé (Linux uniquement)	Oui	Oui	Les <i>administrateurs élevés</i> 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 Administrator, 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 ESXi Server

ESXi Server authentifie les utilisateurs qui accèdent aux hôtes ESXi à l'aide de 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 auprès de Server Administrator sont également des interactions directes avec le processus **vmware-hostd**. Pour vérifier que l'authentification fonctionne correctement pour votre site, effectuez des tâches de base ; par exemple, configurez les utilisateurs, les groupes, les autorisations, les rôles et les attributs utilisateur, ajoutez vos propres certificats et déterminez si vous souhaitez utiliser SSL.





 **REMARQUE : Sur les systèmes exécutant le système d'exploitation VMware ESXi Server, tous les utilisateurs doivent disposer de privilèges d'administrateur pour se connecter à Server Administrator. 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 critiques de votre système, avant d'installer les logiciels OpenManage, attribuez des privilèges d'utilisateur à tous les utilisateurs. Les nouveaux utilisateurs peuvent se connecter au logiciel OpenManage à l'aide des privilèges d'utilisateur de leur système d'exploitation.

-  **PRÉCAUTION** : Pour protéger l'accès aux composants critiques de votre système, vous devez attribuer un mot de passe à chacun des comptes d'utilisateur qui a accès au logiciel OpenManage.
-  **PRÉCAUTION** : Désactivez les comptes Invité sur les systèmes d'exploitation Windows pris en charge afin de protéger l'accès aux composants critiques de votre système. Pensez à renommer les comptes Invité pour empêcher les scripts distants d'activer les comptes à l'aide des noms des comptes Invité 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. Il n'est pas nécessaire de créer de nouveaux utilisateurs dans le logiciel OpenManage.

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



-  **REMARQUE** : Pour exécuter les procédures suivantes, Microsoft Active Directory doit être installé sur votre système. 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. Accédez à **Panneau de configuration** → **Outils d'administration** → **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, effectuez un clic droit sur **Utilisateurs** ou sur le conteneur auquel vous voulez ajouter le nouvel utilisateur et pointez sur **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** (Suivant), puis sur **Finish** (Terminer).
5. Double-cliquez sur l'icône représentant l'utilisateur que vous avez créé.
6. Cliquez sur l'onglet **Member of** (Membre de).
7. Cliquez sur **Ajouter**.
8. Sélectionnez le groupe approprié puis cliquez sur **Add** (Ajouter).
9. Cliquez sur **OK**, puis cliquez de nouveau sur **OK**.

-  **REMARQUE** : Les nouveaux utilisateurs peuvent se connecter à OpenManage avec les privilèges d'utilisateur du groupe et du domaine qui leur ont été attribués.

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

Les privilèges d'accès d'administrateur sont attribués à l'utilisateur connecté en tant que racine. Pour plus d'informations sur la création d'utilisateurs et de groupes d'utilisateurs, consultez la documentation de votre système d'exploitation.

-  **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.

Liens associés :

- [Création d'utilisateurs avec des privilèges d'utilisateur](#)
- [Création d'utilisateurs avec des privilèges d'utilisateur privilégié](#)

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 racine ou équivalent.**

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. Légende concernant l'ajout de la définition du rôle dans Server Administrator

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

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 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**.

Tableau 6. Meilleures pratiques en matière de 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 : localhost 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>*
- Space peut également être utilisé comme délimiteur pour les colonnes au lieu de [Tab]

Création d'utilisateurs Server Administrator pour VMware ESXi 6.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. Entrez les informations de connexion, le nom d'utilisateur, l'identifiant utilisateur (UID) numérique et le mot de passe, en spécifiant que le nom d'utilisateur et l'UID sont facultatifs. Si vous ne spécifiez pas l'UID, vSphere Client attribue l'UID disponible suivant.
5. Pour permettre à un utilisateur d'accéder à l'hôte ESXi via un interpréteur de commandes, sélectionnez **Accorder un accès à l'interpréteur de commandes à cet utilisateur**. Les utilisateurs qui ont uniquement accès à l'hôte via vSphere Client n'ont pas besoin d'accès à l'interpréteur de commandes.
6. Pour ajouter un utilisateur à un groupe, sélectionnez le nom du groupe dans le menu déroulant **Group** (Groupe) puis 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.**


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.

Configuring The SNMP Agent

Server Administrator supports the Simple Network Management Protocol (SNMP—a systems management standard—on all supported operating systems. The SNMP support may or may not be installed depending on your operating system and how the operating system was installed. In most cases, SNMP is installed as part of your operating system installation. An installed supported systems management protocol standard, such as SNMP, is required before installing Server Administrator.

You can configure the SNMP agent to change the community name and to send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as the OpenManage Essentials, perform the procedures described in the following sections.

 **NOTE:** The default SNMP agent configuration usually includes a SNMP community name such as public. For security reasons, you must rename the default SNMP community names. For information about renaming the SNMP community names, see [Changing The SNMP Community Name](#).

 **NOTE:** For OpenManage Essentials to retrieve management information from a system running Server Administrator, the community name used by OpenManage Essentials must match a community name on the system running Server Administrator. For OpenManage Essentials to modify information or perform actions on a system running Server Administrator, the community name used by OpenManage Essentials must match a community name that allows Set operations on the system running Server Administrator. For OpenManage Essentials to receive traps (asynchronous event notifications) from a system running Server Administrator, the system running Server Administrator must be configured to send traps to the system running OpenManage Essentials .

The following procedures provide step-by-step instructions for configuring the SNMP agent for each supported operating system:

- [Configuring the SNMP Agent For Systems Running Supported Windows Operating Systems](#)
- [Configuring the SNMP Agent On Systems Running Supported Red Hat Enterprise Linux](#)
- [Configuring the SNMP Agent On Systems Running Supported SUSE Linux Enterprise Server](#)
- [Configuring the SNMP Agent on Systems Running Supported VMware ESXi 5.X and ESXi 6.X Operating Systems](#)

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

Modification du nom de communauté SNMP

 **REMARQUE :** Vous ne pouvez pas modifier le nom de communauté SNMP dans Server Administrator. Définissez le nom de communauté à l'aide des outils SNMP du système d'exploitation.

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 des **SNMP Service Properties** (Propriétés du Service SNMP) est désactivée.
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 de **SNMP Service Configuration** (Configuration du Service SNMP) s'affiche.
 - 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 des **Propriétés du Service SNMP** s'affiche.
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 de **SNMP Service Configuration** (Configuration du Service SNMP) s'affiche.
 - b. Modifiez le nom de communauté dans la boîte de dialogue **Community Name** (Nom de communauté), puis cliquez sur **OK** .
La fenêtre des **SNMP Service Properties** (Propriétés du Service SNMP) s'affiche.

6. 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.

SNMP Agent Access Control Configuration

The management information base (MIB) branch implemented by Server Administrator is identified by the Object Identifier (OID) 1.3.6.1.4.1.674. Management applications must have access to this branch of the MIB tree to manage systems running Server Administrator.

For Red Hat Enterprise Linux and VMware ESXi operating systems, the default SNMP agent configuration gives read-only access for the *public* community only to the MIB-II *system* branch (identified by the 1.3.6.1.2.1.1 OID) of the MIB tree. This configuration does not allow management applications to retrieve or change Server Administrator or other systems management information outside of the MIB-II *system* branch.

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/snmp, 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`.

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 fonctionnant sous 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`.

Configuring the SNMP agent on systems running supported VMware ESXi 6.X operating systems

Server Administrator supports SNMP traps on VMware ESXi 6.X. If a stand-alone license is only present, SNMP configuration fails on VMware ESXi operating systems. Server Administrator does not support SNMP Get and Set operations on VMware ESXi 6.X as the required SNMP support is unavailable. The VMware vSphere Command-Line Interface (CLI) is used to configure systems running VMware ESXi 6.X to send SNMP traps to a management station.

 **NOTE: For more information about using the VMware vSphere CLI, see 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 la 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.

Using Server Administrator

To start a Server Administrator session, double-click the **Server Administrator** icon on your desktop.

The **Server Administrator Log in** screen is displayed. The default port for Server Administrator is 1311. You can change the port, if required. For instructions on setting up your system preferences, see [Systems Management Server Administration Connection Service and Security Setup](#).

Ouverture et fermeture de session

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

La connexion au système local Server Administrator est uniquement disponible si les composants Web Server de Server Administrator et de Server Instrumentation sont installés sur le système local.

 **REMARQUE : La connexion au système local Server Administrator n'est pas disponible pour les serveurs exécutant XenServer 6.5.**

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 **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 *Management Station Software Installation Guide* (Guide d'installation du logiciel Management Station) à l'adresse dell.com/openmanagemanuals.**

Server Administrator Managed System Login — Using the Desktop Icon


This login is available only if the Server Administrator Web Server component is installed on the system. To log in to Server Administrator to manage a remote system:

1. Double-click the **Server Administrator** icon on your desktop.
2. Type the managed system's IP Address or system name or Fully Qualified Domain Name (FQDN).


 **NOTE:** If you have provided the system name or FQDN, the Server Administrator Web Server host converts the system name or FQDN to the IP address of the managed system. You can also connect by providing the port number of the managed system in the following format: Hostname:Port number, or IP address:Port number.

3. If you are using an Intranet connection, select **Ignore Certificate Warnings**.
4. Select **Active Directory Login** to log in using Microsoft Active Directory authentication. If Active Directory software is not used to control access to your network, do not select **Active Directory Login**. See [Using the Active Directory Login](#).
5. Click **Submit**.

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 Serveur web Server Administrator est installé sur le système. Utilisez cette ouverture de session pour gérer Server Administrator Central Web Server :


1. Double-cliquez sur l'icône **Server Administrator** qui se trouve sur votre bureau. La page d'ouverture de session à distance s'affiche.

 **PRÉCAUTION :** L'écran d'ouverture de session affiche une case à cocher **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 **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 Mozilla Firefox ou Microsoft Internet Explorer, une page d'avertissement intermédiaire peut s'afficher pour indiquer qu'il existe un problème avec le certificat de sécurité. Pour assurer la sécurité du système, il vous est recommandé de générer un nouveau certificat X.509, de réutiliser un certificat X.509 existant ou d'importer une chaîne de certificats 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 des certificats X.509, voir [Gestion des certificats X.509](#).

 **REMARQUE :** Pour assurer la sécurité du système, il vous est recommandé d'importer une chaîne de certificats depuis une autorité de certification (CA). Pour en savoir plus, voir la documentation VMware.

 **REMARQUE** : Si l'autorité de certification du système géré est valide et si le serveur web Server Administrator signale encore une erreur de certificat non fiable, vous pouvez tout de même en faire une autorité de certification 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 d'alignement des certificats pour importer des 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 *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse dell.com/openmanagemanuals.

Connexion directe

L'option 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 **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 unique 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 EMC OpenManage Essentials) 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 (Outils) → Internet Options (Options Internet) → Security (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** (Ajouter ce site Web à la zone).
6. Sous **Security level for this zone** (Niveau de sécurité pour cette zone), cliquez sur **Custom Level** (Personnaliser le niveau).
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 (Précédent et 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 7. 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
Système	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.

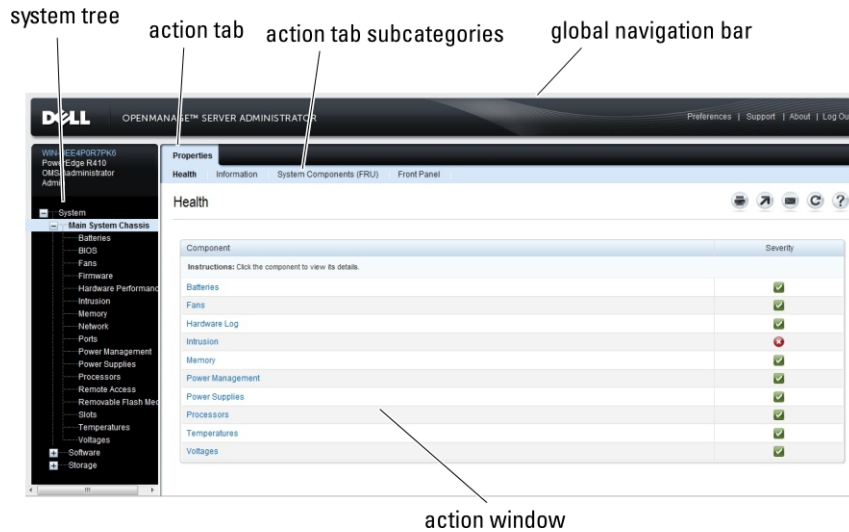


Figure 1. Exemple de page d'accueil de Server Administrator — Système non modulaire

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.

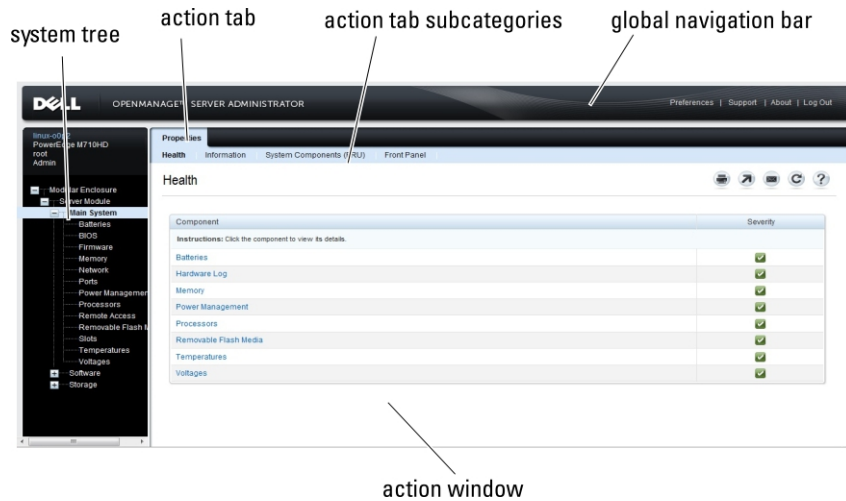


Figure 2. Exemple de page d'accueil de Server Administrator — Système modulaire

Le fait de cliquer sur un objet dans l'arborescence système ouvre une fenêtre d'actions correspondante pour cet objet. Vous pouvez vous déplacer dans 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 zone de données dans la fenêtre d'action qui contient davantage de détails. Par exemple, si vous cliquez sur **Châssis du système principal/Système principal** dans la sous-catégorie **Intégrité** de l'onglet d'action **Propriétés**, cela entraîne la création d'une liste dans laquelle est répertoriée la condition d'intégrité de tous les composants de l'objet Châssis du système principal/Système principal 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 accessible dans l'onglet 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 8. 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	✗	✓
Hardware Performance	✗	✓
Intrusion	✗	✓
Mémoire	✓	✓
Réseau	✓	✓

Fonctions	Système modulaire	Système non-modulaire
Ports		
Power Management (gestion de l'alimentation)		
Processeurs		
Accès à distance		
Média flash amovible		
Emplacements		
Températures		
Tensions		
Enceinte modulaire (Informations sur le châssis et sur CMC)		



Barre de navigation globale

Tous les utilisateurs de ce programme ont accès à la barre de navigation globale et à ses liens.

- Cliquez sur **Préférences** pour ouvrir la page d'accueil **Préférences**. Voir [Utilisation de la page d'accueil Préférences](#).
- Cliquez sur **Support** pour vous connecter au site Web Dell EMC Support.
- Cliquez sur **À propos de** pour afficher la version de Server Administrator et les informations de copyright.
- Cliquez sur **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 **Système de l'enceinte modulaire** → **/Module serveur** les catégories principales de composants du système/module serveur pouvant apparaître sont **Châssis du système principal/Système principal**, **Logiciel** et **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 **Propriétés** (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 9. Indicateurs de condition des composants de système/module de serveur

Description	Icône
	le composant est intègre (normal).
	Le composant présente 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 présente 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** (Imprimer) (), une copie de la fenêtre ouverte s'imprime sur votre imprimante par défaut.
- Si vous cliquez sur **Export** (Exporter) (), 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 **E-mail** (), cela crée un email adressé au destinataire que vous avez spécifié. Pour obtenir des instructions sur la configuration du serveur de messagerie et du destinataire d'e-mail par défaut, voir « Configurer l'utilisateur » et « Préférences système ».
- 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 Exporter, E-mail et Enregistrer sous sont uniquement visibles par les utilisateurs connectés avec des privilèges d'utilisateur privilégié ou d'administrateur. Le bouton Effacer le journal 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.

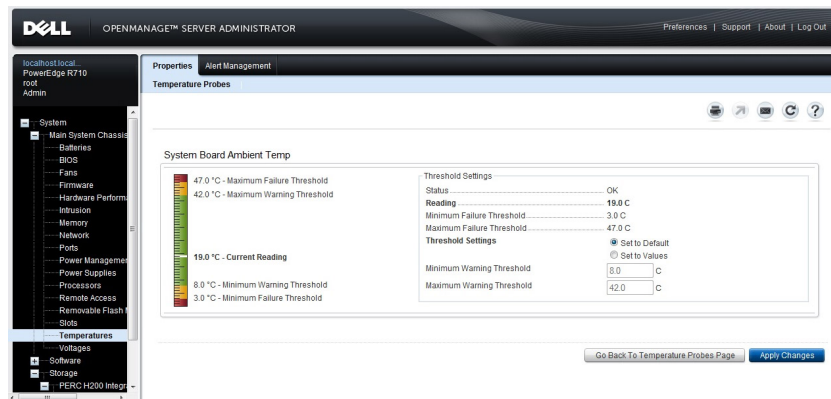


Figure 3. Indicateur de niveau

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 (Préférences) sont les suivantes :

- Paramètres généraux
- Server Administrator

Vous pouvez afficher l'onglet **Préférences** (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 **Préférences** 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 **Préférences** (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.

Préférences du système géré

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

Cliquez sur l'objet Server Administrator pour activer ou désactiver l'accès pour les 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 **Préférences**.

Sous l'onglet **Preferences** (Préférences), 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 : traditionnel et optimisé. Le format par défaut est traditionnel, le format hérité.**

- Active la sauvegarde automatique et l'effacement des entrées du journal ESM.
Par défaut, la fonction est désactivée. L'activation de la fonction vous permet de créer une sauvegarde automatique des journaux ESM. Une fois la sauvegarde créée, les journaux ESM de Server Administrator et les entrées du journal SEL du contrôleur iDRAC/BMC sont effacés. Le processus est répété chaque fois que les journaux sont saturés.

La sauvegarde est enregistrée sur :

Windows : <Install_root>\omsa\log\omsellog.xml

Linux et ESXi : <Install_root>/var/log/openmanage/omsellog.xml

 **REMARQUE : Cette fonction est uniquement disponible sur les systèmes PowerEdge de 10e et 11e générations. Le contrôleur iDRAC offre des fonctionnalités de sauvegarde automatique et de suppression du journal SEL sur les serveurs PowerEdge de 12e génération ou versions ultérieures.**

- Sélectionnez ou désélectionnez les gravités des entrées du journal consignées dans le journal des événements principaux du système d'exploitation. Sélectionnez les valeurs possibles : **Critique**, **Avertissement du journal** ou **Information du journal**.

 **REMARQUE : Par défaut, toutes les options sont sélectionnées. La fonction de filtre de journalisation du système d'exploitation est disponible lorsque le composant filtre de journalisation du système d'exploitation est installé.**

- Sélectionnez **Activer** pour consigner tous les événements de capteurs ESM non surveillés. Lorsque cette fonction est activée, Server Administrator génère des interruptions SNMP, des journaux de système d'exploitation et des alertes pour tous les capteurs non surveillés.
- 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 Systems Management Server Administration et configuration de la sécurité

Configuration des préférences utilisateur et système


La page d'accueil **Préférences** permet de définir les préférences utilisateur et Webserver.

 **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 **Préférences** (Préférences) sur la barre de navigation globale.
La page d'accueil **Préférences** s'affiche.
2. Cliquez sur **General Settings** (Paramètres généraux).
3. Pour ajouter un destinataire de courrier électronique/e-mail pré-sélectionné, saisissez l'adresse e-mail de votre contact désigné pour le service dans le champ **Destinataire**, puis cliquez sur **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 Server Administrator ou le système sur lequel Server Administrator est installé. Utilisez la commande omconfig pour saisir à nouveau l'URL.

Préférences Webserver

Procédez comme suit pour configurer vos préférences Webserver :

1. Cliquez sur **Préférences** (Préférences) sur la barre de navigation globale.
La page d'accueil **Préférences** (Préférences) apparaît.
2. Cliquez sur **General Settings** (Paramètres généraux).
3. Dans la fenêtre **Préférences serveur**, définissez les options souhaitées.
 - Utilisez la fonction **Délai d'expiration de la session (en minutes)** pour définir la durée limite pendant laquelle une session Server Administrator reste active. Sélectionnez **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 **Désactiver** si vous souhaitez désactiver la fonction **Délai d'expiration de la session (en minutes)** de Server Administrator.
 - Le champ **Port HTTPS** indique le port sécurisé de Server Administrator. Le port sécurisé par défaut pour Server Administrator est 1311.
 -  **REMARQUE :** Si vous modifiez le numéro de port en le remplaçant par un numéro non valide ou déjà utilisé, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré. Pour obtenir la liste des ports par défaut, consultez le *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse dell.com/openmanagemanuals.
 - Le champ **Adresse IP à lier à** indique la ou les adresses IP du système géré auxquelles Server Administrator est lié au démarrage d'une session. Sélectionnez **Toutes** pour lier toutes les adresses IP applicables de votre système. Sélectionnez **Spécifique** pour relier une adresse IP spécifique.
 -  **REMARQUE :** Si vous donnez une autre valeur que **All (Toutes)** 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 **Destinataire** spécifie la ou les adresses auxquelles vous souhaitez envoyer des e-mails concernant les mises à jour par défaut. Vous pouvez configurer plusieurs adresses e-mail en les séparant par une virgule.
 - Les champs **Nom du serveur SMTP (ou adresse IP)** et **Suffixe DNS du serveur SMTP** spécifient le protocole SMTP et le suffixe DNS (serveur de noms de domaine) de votre entreprise ou organisation. Pour permettre à Server Administrator d'envoyer des e-mails, 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 **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 **Chiffrement SSL** indique une connexion sécurisée entre le serveur Web et le navigateur. Choisissez les chiffrements qui prennent en charge le serveur Web lors de la configuration. Le service de connexion ne démarre pas si une suite de chiffrement non valide est définie. Par défaut, les éléments suivants sont les valeurs de suite de chiffrement :


TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHANOTE

 **REMARQUE : Si la valeur de chiffrement définie n'est pas valide et que le service de connexion échoue au démarrage, utilisez l'invite de commande CLI ou définissez manuellement les chiffrements valides, puis redémarrez le service de connexion.**

- Le champ **SSL Protocols** (Protocoles SSL) vous permet d'effectuer une configuration à partir des protocoles SSL répertoriés dans le serveur Web pour établir une connexion HTTPS. Les valeurs possibles sont les suivantes : TLSv1 , TLSv1.1 , TLSv1.2 , (TLSv1 , TLSv1.1) , (TLSv1.1 , TLSv1.2) et (TLSv1 , TLSv1.1 , TLSv1.2). Par défaut, la valeur du protocole SSL est définie sur (TLSv1 , TLSv1.1 , TLSv1.2). Les modifications prennent effet après le redémarrage du serveur Web.

 **REMARQUE : Si le protocole n'est pas pris en charge par les configurations par défaut, activez le protocole SSL à partir des paramètres du navigateur.**

- 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 : 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 générez 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.
 - JRE système** : permet d'utiliser le JRE installé sur le système. Sélectionnez la version requise dans la liste déroulante.

 **REMARQUE : Server Administrator ne recommande pas la mise à niveau vers des versions majeures de Java Runtime Environment (JRE) ; elle est limitée aux correctifs de sécurité et aux versions JRE mineures. Pour plus d'informations, consultez les notes de mise à jour de Server Administrator (inclus avec l'application Server Administrator ou disponibles sur Internet à l'adresse dell.com/openmanagemanuals).**

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

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

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

X.509 Certificate Management

 **NOTE: You must be logged in with Administrator privileges to perform certificate management.**

Web certificates are necessary to ensure the identity of a remote system and ensure that information exchanged with the remote system are not viewed or changed by others. To ensure system security, it is recommended that:

- You generate a new X.509 certificate, reuse an existing X.509 certificate or import a certificate chain from a Certification Authority (CA).
- All systems that have Server Administrator installed have unique host names.

To manage X.509 certificates through the **Preferences** home page, click **General Settings**, click the **Web Server** tab, and click **X.509 Certificate**.

The following are the available options:

- **Generate a new certificate** — Generates a new self-signed certificate used for SSL communication between the server running Server Administrator and the browser.
 - ✎ **NOTE: When using a self-signed certificate, most web browsers display an *untrusted* warning as the self-signed certificate is not signed by a Certificate Authority (CA) trusted by the operating system. Some secure browser settings can also block the self-signed SSL certificates. The Server Administrator web GUI requires a CA-signed certificate for such secure browsers.**
- **Certificate Maintenance** — Allows you to generate a Certificate Signing Request (CSR) containing all the certificate information about the host required by the CA to automate the creation of a trusted SSL web certificate. You can retrieve the necessary CSR file either from the instructions on the Certificate Signing Request (CSR) page or by copying the entire text in the text box on the CSR page and pasting it in the CA submit form. The text must be in the Base64-encoded format.
 - ✎ **NOTE: You also have an option to view the certificate information and export the certificate that is being used in the Base64-encoded format, which can be imported by other web services.**
- **Import certificate chain** — Allows you to import the certificate chain (in PKCS#7 format) signed by a trusted CA. The certificate can be in DER or Base64-encoded format.
- **Import a PKCS12 Keystore** — Allows you to import a PKCS#12 keystore that replaces the private key and certificate used in Server Administrator web server. PKCS#12 is public keystore that contains a private key and the certificate for a web server. Server Administrator uses the Java KeyStore (JKS) format to store the SSL certificates and its private key. Importing a PKCS#12 keystore to Server Administrator deletes the keystore entries, and imports a private key and certificate entries to the Server Administrator JKS.
 - ✎ **NOTE: An error message is displayed if you either select an invalid PKCS file or when you type an incorrect password.**

Certificats de serveur SSL

Le serveur Web Server Administrator est configuré pour utiliser le protocole de sécurité standard SSL lors du transfert de données chiffrées sur un réseau. Le protocole SSL repose sur une technologie de chiffrement asymétrique et fournit une communication chiffrée et authentifiée entre clients et serveurs pour prévenir les écoutes illicites sur les réseaux.

Un système SSL peut effectuer les tâches suivantes :

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

Le processus de chiffrement garantit un haut niveau de protection des données. Server Administrator utilise la forme de chiffrement la plus fiable actuellement disponible pour les navigateurs Internet d'Amérique du Nord.

Par défaut, le serveur Web Server Administrator comprend un certificat numérique SSL auto-signé unique. Vous pouvez remplacer le certificat SSL par défaut par un certificat signé par une autorité de certification (AC) reconnue. Une autorité de certification est une entité commerciale qui répond de manière fiable aux normes exigeantes du secteur des technologies de l'information en matière de filtrage, d'identification et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'autorités de certification. Pour lancer le processus d'obtention d'un certificat signé par une autorité de certification, utilisez l'interface Web de Server Administrator afin de générer une Requête de signature de certificat (CSR) accompagnée des informations relatives à votre société. Soumettez ensuite la requête CSR générée à une autorité de certification telle que VeriSign ou Thawte. L'autorité de certification peut être une autorité de certification racine ou autorité de certification intermédiaire. Après réception du certificat SSL signé par une autorité de certification, chargez-le sur Server Administrator.

Le certificat SSL de chacune des instances de Server Administrator à approuver par la station de gestion doit être placé dans le magasin de certificats de la station de gestion. Une fois le certificat SSL installé sur les stations de gestion, les navigateurs pris en charge peuvent accéder à Server Administrator sans avertissements de certificat.

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

Upgrading web server

 **CAUTION: Factory reset is not possible after a web server update. For a factory reset, reinstall the Server Administrator.**

You can upgrade the Apache Tomcat web server, whenever required, using the **omwsupdateutility**, without affecting the Server Administrator functionality. The utility allows upgrade to a minor version of web server, but does not support upgrade to a major version. For example, upgrade from version A.x to A.y is supported, but not A.x to B.x or B.y. Also, using the utility you can move the version of the web server to an earlier version, provided it is a minor version. The utility is saved to the following default location during web server installation:

- On systems running a Windows operating system: `C:\Program Files\Dell\SysMgt\omsa\wsupdate`
- On systems running a Linux operating system: `/opt/dell/srvadmin/lib64/openmanage/wsupdate`

You can download the required version of Tomcat web server package and run the utility from a command prompt. Download the Tomcat web server core distribution package from **tomcat.apache.org**. The distribution package must be a .zip or .tar.gz file; Windows installer wrapper packages are not supported.

To update web server, browse to the **wsupdate** folder and then run the following command:

- On Windows: `omwsupdate.bat [SysMgt folder path] [apache-tomcat.zip/.tar.gz file path]`
- On Linux: `omwsupdate.sh [srvadmin folder path] [apache-tomcat.zip/.tar.gz file path]`

The default **SysMgt** folder path is `C:\Program Files\Dell\SysMgt` and **srvadmin** folder path is `/opt/dell/srvadmin`.

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 *Server Administrator Command Line Interface Guide* (Guide d'utilisation de l'interface de ligne de commande de Server Administrator) à l'adresse **dell.com/openmanagemanuals**.

Services Server Administrator

Le service d'instrumentation Server Administrator 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 ventilateurs 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 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.

 **REMARQUE :** 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 accessible dans l'onglet 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 obtenir des informations détaillées sur le composant Storage Management Service, voir le *Storage Management User's Guide* (Guide d'utilisation de Storage Management) à dell.com/openmanagemanuals.

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. Compte tenu des limitations inhérentes aux systèmes d'exploitation ESXi, certaines fonctionnalités disponibles dans les versions antérieures de Server Administrator ne sont pas disponibles dans cette version.


Les fonctionnalités non prises en charge sur ESXi sont les suivantes :

- 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
- 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 : Des 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 connectés avec des privilèges d'administrateur ont accès aux fonctionnalités système critiques telles que la fonctionnalité d'arrêt disponible dans l'onglet 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 emplacements 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 contrôleur 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

Les trois principaux groupes de composants système de l'objet **Système/Module de serveur** sont les suivants : [Châssis de système principal/Système principal](#), [Logiciel](#) et [Stockage](#). Par défaut, la page d'accueil de Server Administrator est définie sur l'objet **Système** de la vue de l'arborescence système. La plupart des fonctions d'administration peuvent être gérées depuis la fenêtre d'action de l'objet **Système/Module de serveur**. La fenêtre d'action de l'objet **Système/Module de serveur** comporte les onglets suivants, en fonction des privilèges du groupe de l'utilisateur : **Licences**, **Propriétés**, **Arrêt**, **Journaux**, **Gestion des alertes** et **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, la description, l'ID de droit et la date d'expiration de la licence.

 **REMARQUE** : Server Administrator prend en charge la fonction Licences sur les systèmes PowerEdge de 12^e génération et versions ultérieures. Cette fonction est uniquement disponible si la version minimale requise de l'iDRAC, iDRAC 1.30.30, est installée.


 **REMARQUE** : Cette fonction est disponible uniquement si la version minimale requise de l'iDRAC 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 minuteur de surveillance du système d'exploitation est activé dans le BIOS. Pour configurer les options de récupération automatique, le minuteur de 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 la surveillance 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 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 du minuteur de surveillance 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 à cet emplacement, le code BIOS résidant dans cet espace peut être corrompu. Dans la mesure où la fonction de surveillance appelle le BIOS pour déclencher le comportement d'arrêt ou de redémarrage, elle peut ne pas fonctionner correctement. Dans ce cas, vous devez redémarrer le système manuellement. Le minuteur de surveillance 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 **Arrêt**, 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 la liste de tous les événements associés aux composants matériels 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 80 % de sa capacité. Sur les systèmes PowerEdge 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 %.

 **REMARQUE : L'activation de la fonction Sauvegarde automatique et suppression des entrées du journal ESM vous permet de créer une sauvegarde automatique des journaux ESM. Cette fonction n'est disponible que sur les serveurs PowerEdge 10e et 11e générations. Le contrôleur iDRAC offre des fonctionnalités de sauvegarde automatique et de suppression du journal SEL sur les systèmes PowerEdge de 12e génération et versions ultérieures. Seule la dernière version du fichier de sauvegarde XML est disponible aux emplacements susmentionnés.**

- 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/openmanagemanuals.**

- 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 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 **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.

- **Interruption de test SNMP** envoie l'interruption à la destination sélectionnée à partir de la liste affichée de destinations configurées. Le composant SNMP de Server Administrator doit être installé pour l'envoi de l'interruption de test. L'administrateur doit configurer les adresses IP/FQDN dans le service SNMP du système d'exploitation ou le fichier de configuration pour l'obtention de la liste des destinations d'interruption.

 **REMARQUE : Cette fonction n'est pas prise en charge sur VMware ESXi.**

- La fenêtre **Enable SNMP Traps** (Activer les interruptions SNMP) permet de configurer les paramètres d'un composant à l'aide d'une case à cocher et d'un bouton radio. La sélection d'un bouton radio modifie l'état de la case à cocher correspondante alors que la désélection du bouton radio modifie également l'état de la case à cocher correspondante.

 **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 (Paramètres de système avancés) → Advanced Recovery (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 Gestion de session 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](#)
- [Microprogramme](#)
- [Performances matérielles](#)
- [Intrusion](#)
- [Mémoire](#)
- [Réseau](#)
- [Ports](#)
- [Gestion de l'alimentation](#)
- [Blocs d'alimentation](#)
- [Processeurs](#)
- [Accès à distance](#)
- [Média flash amovible](#)
- [Logements](#)
- [Températures](#)
- [Tensions](#)

 **REMARQUE** : L'option Blocs d'alimentation n'est pas disponible sur PowerEdge 1900. Les fonctionnalités Surveillance des blocs d'alimentation et Surveillance de l'alimentation sont uniquement disponibles 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 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. La fenêtre d'action de l'objet **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 **Propriétés** (Propriétés), vous pouvez :

- Afficher l'intégrité ou la condition des composants matériels et des capteurs. Une icône [Voyants de condition du composant du système/serveur](#) se trouve en regard du nom de chaque composant répertorié.  indique qu'un composant est intègre (normal).  indique que le composant présente une condition d'avertissement (non critique) et qu'il doit être vérifié.  indique qu'un composant présente une condition critique/défaillante et qu'il nécessite une intervention immédiate.  indique que la condition d'intégrité d'un composant est inconnue. Les composants surveillés disponibles comprennent :

- [Batteries](#)
- [Ventilateurs](#)
- [Journal du matériel](#)
- [Intrusion](#)
- [Réseau](#)
- [Power Management \(gestion de l'alimentation\)](#)
- [Blocs d'alimentation](#)
- [Processeurs](#)
- [Températures](#)
- [Tensions](#)

 **REMARQUE : Les batteries sont uniquement prises en charge sur les systèmes PowerEdge de 10e génération. Les Blocs d'alimentation ne sont pas disponibles sur PowerEdge 1900. La Gestion de l'alimentation est prise en charge sur certains systèmes PowerEdge de 10e génération. Les fonctionnalités Surveillance des blocs d'alimentation et Surveillance de l'alimentation sont uniquement disponibles 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.**

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

- Affichez des informations sur les attributs du châssis de système principal tels que le nom d'hôte, la version de l'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) à 11 chiffres du numéro de service du système. Lorsque vous appelez le support technique Dell EMC, vous pouvez entrer le code 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 l'indication d'une session KVM distante dans le sous-onglet **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 : **Propriétés** (Propriétés) et **Alert Management** (Gestion des alertes).

Propriétés

Sous-onglet : batteries

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

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.
- Configurer les alertes que vous souhaitez voir apparaître en cas d'avertissement ou d'événement critique/d'échec au sujet de la batterie.

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, comme 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 :

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

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, 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'Hyper-Threading 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 les ports de réseau LAN supplémentaires sur la carte mère. Et vous pouvez 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.


Sur les serveurs PowerEdge de 12e génération et les systèmes ultérieurs, les fonctionnalités configurables du BIOS sont regroupées en catégories spécifiques, dont : Menu de débogage, Informations sur le système, Paramètres de mémoire, Paramètres du processeur, Paramètres SATA, Paramètres d'amorçage, Paramètres des options d'amorçage, Paramètres réseau, Périphériques intégrés, Désactivation des emplacements, Communications série, Paramètres du profil du système, Sécurité système et Paramètres divers. Par exemple, sur la page **Paramètres du BIOS du système**, lorsque vous cliquez sur le lien **Paramètres de mémoire**, les fonctionnalités qui correspondent à la mémoire du système s'affichent. Vous pouvez afficher ou modifier les paramètres en naviguant vers les catégories respectives.

 **REMARQUE : La catégorie Amorçage ponctuel n'est pas prise en charge sur les systèmes PowerEdge de 13ème génération.**

Les fonctionnalités configurables du BIOS sont regroupées en catégories spécifiques, dont : Menu de débogage, Informations sur le système, Paramètres de mémoire, Paramètres du processeur, Paramètres SATA, Paramètres d'amorçage, Paramètres des options d'amorçage, Paramètres réseau, Périphériques intégrés, Désactivation des emplacements, Communications série, Paramètres du profil du système, Sécurité système et Paramètres divers. Par exemple, sur la page **Paramètres du BIOS du système**, lorsque vous cliquez sur le lien **Paramètres de mémoire**, les fonctionnalités qui correspondent à la mémoire du système s'affichent. Vous pouvez afficher ou modifier les paramètres en naviguant vers les catégories respectives.

Vous pouvez définir un mot de passe de configuration du BIOS sur la page **Sécurité système**. Si vous avez défini le mot de passe de configuration, saisissez-le pour activer et modifier les paramètres du BIOS. Sinon, les paramètres du BIOS apparaîtront en mode Lecture seule. Redémarrez le système après avoir défini le 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 être inexactes dans le cas de NIC intégrés. L'utilisation de l'écran de configuration du BIOS pour activer ou désactiver les NIC peut avoir des effets 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.**

Cycle d'alimentation complet : cette nouvelle fonctionnalité permet aux administrateurs de serveurs d'exécuter un cycle d'alimentation sur le périphérique à l'aide de l'interface GUI ou CLI d'OpenManage. La fonctionnalité **Cycle d'alimentation complet** permet à l'administrateur d'exécuter un cycle d'alimentation CC suivi d'un cycle d'alimentation CA.

Le cycle d'alimentation CC redémarre le serveur, mais les périphériques auxiliaires ne sont pas interrompus. Le cycle d'alimentation CA redémarre les périphériques auxiliaires et connecte l'utilisateur au serveur.

La fonctionnalité **Cycle d'alimentation complet** permet d'exécuter un cycle d'alimentation sur les périphériques suivants :

- Serveur
- BMC/iDRAC
- CPLD
- Capteurs
- LCD
- Unité remplaçable sur site
- Titan
- Carte fille réseau

Configuration du cycle d'alimentation CA virtuel

Pour définir le cycle d'alimentation CA virtuel :

1. Dans la fenêtre Server Administrator, développez **Système** → **Châssis de système principal**.
2. Cliquez sur **BIOS**.
La fenêtre **Propriétés BIOS** s'affiche.
3. Cliquez sur l'onglet **Configuration**.
La fenêtre **Paramètres du BIOS du système** s'affiche.
4. Cliquez sur le lien **Paramètres divers**.
5. Sous **Demande de cycle d'alimentation**, sélectionnez **CA virtuel**.
6. Cliquez sur **Appliquer**.

 **REMARQUE : Redémarrez le serveur pour changer le paramètre de cycle d'alimentation.**

Ventilateurs

Cliquez sur l'objet **Ventilateurs** pour gérer les ventilateurs de votre système. Server Administrator surveille la condition de chaque ventilateur du système en mesurant le nombre de tours par minute des ventilateurs. Les capteurs de ventilateur indiquent les tours par minute au service d'instrumentation de Server Administrator.

Lorsque vous sélectionnez Ventilateurs dans l'arborescence de périphérique, des détails apparaissent dans la zone de données du volet de droite de la page d'accueil de Server Administrator. La fenêtre d'action de l'objet Ventilateurs peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **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** (Gestion des alertes), 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.
- Définissez les niveaux des seuils d'alerte des ventilateurs.

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).

Propriétés

Sous-onglet : Informations

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

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

Tableau 10. 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.

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 le 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 :

Propriétés et 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** (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'intrusion 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 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 : **Propriétés** (Propriétés) et **Alert Management** (Gestion des alertes).

Propriétés

Sous-onglet : Memory (Mémoire)

Sous l'onglet **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 offrent 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 renvoie 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.

Réseau

Cliquez sur l'objet **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. 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 physiques 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.**

Dans le système d'exploitation ESXi, le périphérique réseau est considéré comme un groupe. Par exemple, l'interface Ethernet virtuelle utilisée par la console de services (vswif) et l'interface réseau virtuelle qui est utilisée par le périphérique vmknic sur ESXi.

 **REMARQUE : Server Administrator prend uniquement en charge l'inventaire des interfaces réseau physiques et de leurs propriétés. Server Administrator ne prend pas en charge l'inventaire des interfaces logiques tels que les VLAN et les dispositifs liés.**

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

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, 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.**

 **REMARQUE : Sur les systèmes exécutant les systèmes d'exploitation Linux avec les versions de noyau antérieure à 3.10, la vitesse de l'interface d'équipe n'est pas affichée.**

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 CMC connectés à des serveurs lames ne sont pas énumérés par Server Administrator.**


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

Sous-onglet : Informations

Propriétés

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

Power Management (gestion de l'alimentation)

 **REMARQUE : Les fonctions Surveillance des blocs d'alimentation et 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 **Blocs d'alimentation** pour gérer les blocs d'alimentation de votre système. Server Administrator surveille la condition des blocs d'alimentation, y compris la redondance, pour assurer que le bloc d'alimentation installé sur votre système fonctionne correctement.

La fenêtre d'action de l'objet Blocs d'alimentation peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **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 de bloc d'alimentation, notamment la version micrologicielle du bloc d'alimentation et la puissance de sortie maximale.
- 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 **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 : **Propriétés** et **Gestion des alertes**.

Sous-onglet : Informations

Propriétés

Sous l'onglet **Propriétés**, 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 **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 : 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 : **Propriétés** (Propriétés), **Configuration** et **Users** (Utilisateurs).

Sous-onglet : Informations

Propriétés

Sous l'onglet **Propriétés** (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 :

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).

Média flash amovible

Cliquez sur l'objet **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 **Média flash amovible** comporte l'onglet **Propriétés**.

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, 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** (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 du média flash amovible 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 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.

Emplacements

Cliquez sur l'objet **Emplacements** 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 Emplacements comporte l'onglet **Propriétés**.

Propriétés

Sous-onglet : Informations

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


Températures

Cliquez sur l'objet **Températures** pour gérer la température de votre système afin d'éviter l'endommagement thermique des composants internes de votre système. Server Administrator surveille la température à plusieurs endroits du châssis de votre système pour que les températures dans le châssis ne soient pas trop élevées.

La fenêtre d'action de l'objet **Températures** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Sous-onglet : Temperature Probes (Capteurs de température)

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 **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 **Tensions** peut comporter les onglets suivants, en fonction des privilèges de groupe de l'utilisateur : **Propriétés** et **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 **Propriétés** (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 **Système d'exploitation** pour afficher des informations de base relatives à votre système d'exploitation. La fenêtre d'action de l'objet Système d'exploitation comporte l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, 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 : **Propriétés**.

Propriétés

Sous-onglet : Health (Intégrité)

Sous l'onglet **Propriétés**, 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](#)

General settings

Click the **General Settings** object to set user and DSM SA Connection Service (web server) preferences for selected Server Administrator functions. The General Settings object action window has the following tabs, depending on the user's group privileges: **User** and **Web Server**.

Subtab: Properties

User

Under the **User** tab, you can set user preferences, such as the home page appearance and the default email address for the **E-mail** button.

- **Web Server**
- **Subtabs: Properties | X.509 Certificate**

Under the Web Server tab, you can:

- Set DSM SA Connection Service preferences. For instructions on configuring your server preferences, see [Dell EMC Systems Management Server Administration Connection Service and Security Setup](#).
- Configure the SMTP server address and Bind IP address in either the IPv4 or IPv6 addressing mode.

- Perform X.509 certificate management by generating a new X.509 certificate, reusing an existing X.509 certificate, or importing a certificate chain from a Certification Authority (CA). For more information about certificate management, see [X.509 Certificate Management](#).

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. La fenêtre d'action de l'objet **Server Administrator** peut comporter l'onglet suivant, selon les privilèges du groupe de l'utilisateur : **Préférences**.

Sous-onglets : Configuration de l'accès

Préférences

Sous l'onglet **Préférences**, vous pouvez activer ou désactiver l'accès pour les utilisateurs ayant des privilèges d'utilisateur ou d'utilisateur privilégié.

Working with remote access controller

The systems baseboard management controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) monitors the system for critical events by communicating with various sensors on the system board and sends alerts and log events when certain parameters exceed their preset thresholds. The BMC/iDRAC supports the industry-standard Intelligent Platform Management Interface (IPMI) specification, enabling you to configure, monitor, and recover systems remotely.

 **NOTE: The Integrated Dell Remote Access Controller (iDRAC) is supported on the 10th generation PowerEdge and later systems.**

The DRAC is a systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for the systems.

By communicating with the system's baseboard management controller (BMC)/Integrated Dell Remote Access Controller (iDRAC), the DRAC can be configured to send you email alerts for warnings or errors related to voltages, temperatures, and fan speeds. The DRAC also logs event data and the most recent failure screen (available only on systems running Microsoft Windows operating system) to help you diagnose the probable cause of a system failure.

The Remote Access Controller provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Controller also provides alert notification when a system is down and allows you to remotely restart a system. Also, the Remote Access Controller logs the probable cause of system fails and saves the *most recent crash screen*.

You can log in to the Remote Access Controller through the Server Administrator home page or by directly accessing the controller's IP address using a supported browser.

When using the Remote Access Controller, you can click **Help** for more detailed information about the specific window you are viewing. Remote Access Controller help is available for all windows accessible to the user based on the user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

 **NOTE: For more information about the BMC, see the *Dell EMC OpenManage Baseboard Management Controller User's Guide* at dell.com/systemsecuritymanuals.**

 **NOTE: For detailed information on configuring and using the iDRAC, see the *Integrated Dell Remote Access Controller User's Guide* at dell.com/systemsecuritymanuals.**

The following table lists the graphical user interface (GUI) field names and the applicable system, when Server Administrator is installed on the system.

Table 11. GUI Field Names And The Applicable System

GUI Field Name	Applicable System
Modular Enclosure	Modular system
Server Modules	Modular system
Main System	Modular system
System	Non-modular system
Main System Chassis	Non-modular system

For more information on the systems support for remote access devices, see the *Dell EMC Systems Software Support Matrix* available at dell.com/openmanagemanuals.

Server Administrator allows remote, in-band access to event logs, power control, and sensor status information and provides the ability to configure the BMC/iDRAC. To manage BMC/iDRAC and DRAC through the Server Administrator graphical user interface (GUI), click the **Remote Access** object, which is a subcomponent of the **Main System Chassis/Main System** group.

You can perform the following tasks:

- [Viewing Basic Information](#)
- [Configuring The Remote Access Device To Use A LAN Connection](#)
- [Configuring The Remote Access Device To Use A Serial Over LAN Connection](#)
- [Configuring The Remote Access Device To Use A Serial Port Connection](#)
- [Additional Configuration For iDRAC](#)
- [Configuring Remote Access Device Users](#)
- [Setting Platform Event Filter Alerts](#)

You can view BMC/iDRAC or DRAC information based on which hardware is providing the remote access capabilities for the system. The reporting and configuration of BMC/iDRAC and DRAC can also be managed using the `omreport/omconfig chassis remoteaccess` command-line interface (CLI) command.

In addition, the Server Administrator Instrumentation Service allows you to manage the Platform Event Filters (PEF) parameters and alert destinations.

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 :

- Activer le NIC (Sélectionnez cette option pour le regroupement des cartes réseau.)

 **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 versions antérieures 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).

 **REMARQUE :** L'option **Dedicated** est disponible lorsqu'il existe une licence iDRAC7 Enterprise valide. 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
- Nouvelle clé de cryptage

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 plus d'informations sur la gestion de licences, voir le *Dell License Manager User's Guide* (Guide d'utilisation de Dell License Manager) disponible sur le site dell.com/openmanagemanuals.

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.
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.**

Setting Platform Event Filter Alerts

To configure the most relevant BMC features, such as Platform Event Filter (PEF) parameters and alert destinations using Server Administrator Instrumentation Service:

1. Cliquez sur l'objet **System**.
2. Cliquez sur l'onglet **Alert Management**.
3. Cliquez sur **Platform Events**.

The **Platform Events** window allows you to take individual action on specific platform events. You can select those events for which you want to take shutdown actions and generate alerts for selected actions. You can also send alerts to specific IP address destinations of your choice.

 **NOTE: You must be logged in with Administrator privileges to configure the BMC PEF Alerts.**

 **NOTE: The Enable Platform Event Filters Alerts setting disables or enables PEF alert generation. It is independent of the individual platform event alert settings.**


 **NOTE: System Power Probe Warning and System Power Probe Failure are not supported on the PowerEdge systems without PMBus support although Server Administrator allows you to configure them.**


4. Choisissez l'événement de plateforme pour lequel vous souhaitez prendre des actions d'arrêt ou générer des alertes pour des actions sélectionnées et cliquez sur **Set Platform Events**.

The Set **Platform Events** window allows you to specify the actions to be taken if the system is to be shut down in response to a platform event.

5. Select one of the following actions:

- **None**
- **Reboot System**
Shuts down the operating system and initiates system startup, performing BIOS checks and reloading the operating system.
- **Power Off System**
Turns off the electrical power to the system.
- **Power Cycle System**
Turns the electrical power to the system off, pauses, turns the power on, and reboots the system. Power cycling is useful when you want to reinitialize system components such as hard drives.
- **Power Reduction**
Throttles the CPU.

 **CAUTION: If you select a Platform Event shutdown action other than None or Power Reduction, your system shuts down forcefully when the specified event occurs. This shutdown is initiated by firmware and is done without first shutting down the operating system or any running applications.**

 **NOTE: Power reduction is not supported on all systems. Power Supply Monitoring and Power Monitoring features are available only for systems that have two or more redundant, hot-swappable power supplies installed. These features are unavailable for permanently installed, non-redundant power supplies that lack power management circuitry.**

6. Select the **Generate Alert** check box for the alerts to be sent.

 **NOTE: To generate an alert, you must select both Generate Alert and the Enable Platform Events Alerts settings.**

7. Click **Apply**.

8. Click **Apply to Platform Events Page** to go back to the **Platform Event Filters** window.

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**.

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 e-mail 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 *Server Administrator Command Line Interface User's Guide* (Guide d'utilisateur de l'interface de ligne de commande de Server Administrator) à l'adresse dell.com/openmanagemanuals.



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 12. Boutons de tâche des fenêtres des journaux

Nom	Description
Imprimer	Pour imprimer une copie du journal sur votre imprimante par défaut .
Exportation	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.
Email (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 [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 PowerEdge de 11e génération, 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 journal atteint une capacité de 100 pourcent. 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. Chaque composant répertorié dans les journaux possède une icône de voyant d'état en regard de son nom. Le tableau suivant répertorie les voyants d'état.

Tableau 13. Voyant d'état de journal du matériel

État	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.
Une croix 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 %. Assurez-vous de pouvoir supprimer le journal du matériel lorsqu'il atteint une capacité de 80 %. Si le journal atteint une capacité de 100 %, les derniers événements sont supprimés du journal.

Pour effacer le journal du matériel, cliquez sur le lien **Effacer le journal** de la page **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.**

 **REMARQUE : OMSA peut envoyer des interruptions SNMP en double ou journaliser des événements en double sur la page du journal des alertes ou dans le fichier journal du système d'exploitation. La duplication des interruptions et les événements est enregistrée lorsque les services OMSA sont redémarrés manuellement ou lorsque le capteur de périphérique indique encore un état anormal lors du démarrage des services OMSA après un redémarrage du système d'exploitation.**

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/openmanagemanuals.

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.**

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.

Setting Alert actions in Windows Server to Execute Applications

In windows, the **Interactive Services Detection** is disabled by default. The **Interactive Services Detection** must be activated in **Regedit** to enable the executable applications.


To enable the **Interactive Service Detection** follow the steps mentioned below:

1. Modifying the **NolteractiveServices**
 1. Open **Regedit**.
 2. Navigate to `HKLM\SYSTEM\CurrentControlSet\Control\Windows\`.
 3. Right-click **NolteractiveServices** and then click **Modify**.

4. In **Value Data** enter **0** and click **OK**.
5. Close **Regedit**
6. To add the user to a group, select the group name from the **Group** drop-down menu and click **Add**.
7. Click **OK**.
2. Enabling the **Interactive Service Detection**
8. Open **Services.msc**.
9. Navigate to **Interactive Service Detection**.
10. Right-click **Interactive Service Detection** and then click **Properties**.
11. In the **General** tab, change the **Startup Type** to **Automatic** and click **Apply**.
12. In Service Status click **Start**.
3. Allowing the service to interact
13. Navigate to **DSM SA Data Manager**, right-click and then click **Properties**.
14. In the **Logon** tab, enable **Allow service to interact with desktop** and click **Apply**.
15. Click **OK**.

Restart **DSM SA Data Manager** to enable the **Interactive Service Detection**.

Interactive application - Examples of interactive applications are applications with a graphical user interface (GUI) or that prompt the user for input in some way such as the pause command in a batch file.

 **NOTE: To view the interactive application, a pop up message interactive Services Detection is displayed with the message A program running on this computer is trying to display a message, click View the message to proceed.**

Messages d'alertes de filtre 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 14. 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.

Événement	Description
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.
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.

Dépannage

Échec du service de connexion

Sur Red Hat Enterprise Linux, lorsque `SELinux is set to enforced mode`, le service de connexion Systems Management Server Administration (SM SA) ne parvient pas à démarrer. Effectuez l'une des opérations suivantes et démarrez ce service :

- Définissez SELinux sur le mode `Disabled` ou `Permissive`.
- Définissez la propriété SELinux `allow_execstack` sur l'état **ON**. Exécutez la commande suivante :

```
setsebool allow_execstack on
```
- Modifiez le contexte de sécurité du service de connexion SM SA. 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 ESXi. Pour en savoir plus sur l'activation des services Server Administrator sur le système VMware ESXi, consultez le *Server Administrator Installation Guide* (Guide d'installation de Server Administrator), disponible à l'adresse dell.com/openmanagemanuals.
- Le service SFCBD (small footprint CIM broker daemon) du système VMware 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 configurée dans le système géré. Pour en savoir plus sur cette fonction, consultez le *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse dell.com/openmanagemanuals.
- Un échec d'authentification se produit lors de la connexion à un système d'exploitation VMware ESXi 5.0 qui peut 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 défectueuse 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\SystemManagement**.
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 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 15. Services 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 en mesure de se connecter à Server Administrator et de réaliser des opérations via l'interface utilisateur Web. Cependant, l'interface CLI peut encore être 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 fournisseurs SNMP et CIM de Server Administrator d'effectuer une mise à jour des logiciels à distance à l'aide de System Management Console et Dell IT Assistant (ITA).	Les mises à jour de logiciels ne sont réalisables qu'à l'aide d'ITA. Cependant, les mises à jour peuvent être effectuées localement et à l'extérieur de Server Administrator à l'aide de packages de mise à jour Dell (DUP) individuels. Les mises à jour peuvent encore être réalisées à l'aide d'outils tiers (par exemple, MSSMS, Altiris et Novell ZENworks).	Redémarrer le service	Avertissement

 **REMARQUE : Server Administrator peut envoyer des interruptions SNMP en double ou consigner des événements en double sur la page Journal des alertes ou dans le fichier journal du système d'exploitation. Les événements et les interruptions en double sont enregistrés lorsque les services Server Administrator sont redémarrés manuellement ou lorsque le capteur d'appareil indique un état anormal lors du démarrage des services Server Administrator après un redémarrage du système d'exploitation.**

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
 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 Server Administrator (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 service s'exécute sur le système géré.)	Interface Data Engine Linux SNMP	Les demandes SNMP get/set/trap ne fonctionnent pas à partir d'une station de gestion.	Redémarrer le service	Critique
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

Forum aux questions

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

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

1. **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.

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

Connectez-vous au **site : dell.com/support** → Logiciels et Sécurité → Enterprise System Management → OpenManage Server Administrator.

Toutes les versions disponibles de Server Administrator sont affichées sur la page.


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

Une fois que vous êtes connecté à Server Administrator, sélectionnez **Propriétés → Résumé**. La version de Server Administrator installée sur votre système apparaît dans la colonne **Gestion des systèmes**.

4. **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. Sélectionnez **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 vous modifiez le numéro de port en le remplaçant par un numéro non valide ou déjà utilisé, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré. Pour obtenir la liste des ports par défaut, voir le document *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse dell.com/openmanagemanuals.**

5. **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.

6. **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.

7. **Le protocole SNMP est-il requis pour la découverte ITA, l'inventaire et les mises à jour logicielles sur les 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 s'effectuent via une session SSH et un FTP sécurisé ; en outre, des autorisations/informations d'identification de niveau root (racine) sont requises pour cette action discrète et exigées lorsque l'action est configurée ou demandée. Les informations d'identification 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 informations d'identification 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 fichiers d'un endroit

quelconque (par exemple, 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 ports utilisés.

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

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

9. **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 l'exception du tiret) sont également non valides. Utilisez uniquement des lettres sensibles à la casse et des chiffres.

10. **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 d'octroyer un 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 la section « Using Microsoft Active Directory » (Utilisation de Microsoft Active Directory) du document *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse dell.com/openmanagemanuals.

11. **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 :

```
auth required pam_stack.so service=system-auth auth required /lib64/security/pam_nologin.so account required pam_stack.so service=system-auth
```

12. **Les alertes de Server Administrator ne s'affichent pas dans l'interruption SNMP. Comment configurer l'activation des interruptions SNMP ?**

Suivez les étapes de configuration SNMP pour activer les alertes Server Administrator :

- `esxcli system snmp set --communities public`
- `esxcli network firewall ruleset set --ruleset-id snmp --allowed-all true`
- `esxcli network firewall ruleset set --ruleset-id snmp --enabled true`
- `esxcli system snmp set -t <target_ip>@162/public`
- `esxcli system snmp set --enable true`