Dell OpenManage Server Administrator Version 7.0

Guide d'utilisation

Remarques et précautions

REMARQUE : une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre ordinateur.

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

Marques utilisées dans ce document : Dell™, le logo DELL, PowerEdge™, PowerVault™ et OpenManage™ sont des marques de Dell Inc. Microsoft®, Windows®, Internet Explorer®, Active Directory® et Windows Server® sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. EMC® est une marque déposée de EMC Corporation. Java® est une marque déposée d'Oracle et/ou ses filiales. Novell® et SUSE® sont des marques déposées de Novell, Inc. aux États-Unis et dans d'autres pays. Red Hat® et Red Hat Enterprise Linux® sont des marques déposées de Red Hat, Inc. aux États-Unis et dans d'autres pays. VMware® est une marque déposée et ESX Server™ est une marque de VMware Inc aux États-Unis et/ou dans d'autres juridictions. Mozilla® et Firefox® sont des marques déposées de Mozilla Foundation. Citrix®, Xen®, XenServer® et XenMotion® sont des marques déposées ou des marques de Citrix Systems, Inc. aux États-Unis et/ou dans d'autres pays.

Server Administrator comprend des logiciels développés par Apache Software Foundation (**www.apache.org**). Server Administrator utilise la bibliothèque OverLIB JavaScript. Cette bibliothèque est disponible sur **www.bosrup.com**.

D'autres marques et noms commerciaux peuvent être utilisés dans cette publication pour faire référence aux entités revendiquant la propriété de ces marques ou de ces noms de produits. Dell Inc. rejette tout intérêt propriétaire dans les marques et les noms commerciaux autres que les siens.

2012 - 03

Table des matières

1

Introduction

Présentation

Dell OpenManage Server Administrator (OMSA) fournit une solution de gestion de systèmes un-à-un complète, pouvant être utilisée de deux façons : depuis une interface utilisateur graphique (GUI) intégrée Web ou depuis une interface de ligne de commande (CLI) via le système d'exploitation. Server Administrator, conçu pour les administrateurs système, leur permet de gérer les systèmes localement et à distance sur un réseau. Il leur permet également de se concentrer sur la gestion de l'ensemble de leur réseau grâce à une gestion de systèmes un-à-un complète.

Server Administrator peut être utilisé avec un système autonome, un système ayant des unités de stockage réseau connectées dans un châssis séparé ou un système modulaire composé d'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 permet de gérer et d'administrer facilement des systèmes locaux et distants via un ensemble complet de services de gestion intégrés. Server Administrator est le seul à être installé sur le système géré. Il est accessible à la fois localement et à distance depuis la page d'accueil de **Server Administrator**. Les systèmes surveillés à distance sont accessibles par numérotation, LAN ou des connexions sans fil. Server Administrator assure la sécurité de ses connexions de gestion par contrôle d'accès basé sur le rôle (RBAC), l'authentification et le cryptage SSL.

Installation

Vous pouvez installer Server Administrator à l'aide du DVD *Dell Systems Management Tools and Documentation*. Le DVD fournit un programme de configuration pour installer, mettre à niveau et désinstaller les composants logiciels de Server Administrator, du système géré et de la station de gestion. Vous pouvez également installer Server Administrator sur plusieurs systèmes en réalisant une installation automatique sur un réseau.

Le programme d'installation de Dell OpenManage fournit des scripts d'installation et des paquetages RPM pour installer et désinstaller Dell OpenManage Server Administrator et d'autres composants du logiciel Managed System sur votre système géré. Pour en savoir plus, voir le *Guide d'installation de Dell OpenManage Server Administrator* et le *Guide d'installation du logiciel de la station de gestion Dell OpenManage* à l'adresse **support.dell.com/manuals**.

REMARQUE : Lorsque vous installez des progiciels open source depuis le DVD *Dell Systems Management Tools and Documentation*, les fichiers de licence correspondant sont automatiquement copiés sur le système. Lors de la suppression de ces progiciels, les fichiers correspondants sont également supprimés.

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

Mise à jour de composants système particuliers

Pour mettre à jour des composants système particuliers, utilisez les progiciels Dell Update Packages spécifiques aux composants. Utilisez le DVD *Dell Server Updates* (Mises à jour de serveur Dell) pour consulter le rapport de version complet et mettre à jour la totalité d'un système. Server Update Utility est une application sur DVD-ROM qui sert à identifier et appliquer des mises à jour conçues pour votre système. Server Update Utility peut être téléchargé à partir du site **support.dell.com**.

Consultez le *Guide d'utilisation de Server Update Utility* pour plus d'informations sur la manière d'obtenir et d'utiliser Server Update Utility (SUU) pour mettre à jour vos systèmes Dell ou pour afficher les mises à jour disponibles pour tout système répertorié dans l'espace de stockage.

Storage Management Service

Storage Management Service (Service de gestion de stockage) fournit des informations de gestion de stockage sur un écran graphique intégré.

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

Service d'instrumentation

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

Le contrôleur Remote Access Controller fournit une solution de gestion de système à distance complète, dédiée aux systèmes dotés du contrôleur Dell Remote Access Controller (DRAC) ou du contrôleur de gestion de la carte mère (BMC)/solution Integrated DellRemote Access Controller (iDRAC). Remote Access Controller permet d'accéder à distance à un système inutilisable et vous permet ainsi de réparer et de reconnecter ce système aussi vite que possible. Remote Access Controller permet aussi de signaler quand un système est éteint et de le redémarrer à distance. Remote Access Controller journalise également la cause probable des pannes du système et enregistre l'écran de panne le plus récent.

Journaux

Server Administrator affiche les journaux des commandes émises vers ou par le système, des événements matériels contrôlés et des alertes du système. Vous pouvez afficher les journaux sur la page d'accueil, les imprimer ou les enregistrer comme rapports, puis les envoyer par e-mail à un contact de service désigné.

Nouveautés de cette version

Points forts de cette version de OpenManage Server Administrator :

- Prise en charge complémentaire des systèmes d'exploitation suivants :
  - VMware ESXi 5.0 FP1
  - SUSE Enterprise Linux 11 SP2 x86_64

  REMARQUE : Microsoft Windows 2003 n'est pas pris en charge sur les systèmes yx2x.
- Prise en charge supplémentaire des navigateurs suivants:
  - Internet Explorer 9.0
  - Mozilla Firefox 6.0 et 7.0
- Prise en charge supplémentaire des systèmes *yx2x*
- Augmentation de 480 à 720 secondes de la limite du registre d'horloge de la surveillance du système de restauration automatique (ASR).
- Regroupement des paramètres BIOS sous des catégories spécifiques sur la page des paramètres BIOS.
- Quatre nouveaux événements de plateforme supplémentaires pour les cartes modulaires Dual SD internes :
  - Condition critique de la carte du module SD interne double
  - Condition d'avertissement de la carte du module SD interne double
  - Perte de redondance de la carte du module SD interne double
  - Absence de la carte du module SD interne double

  Pour plus d'informations, voir Événements d'alerte PEF.
- Possibilité de sélectionner des réseaux primaire et de basculement pour la NIC de gestion à distance (iDRAC7) des systèmes yx2x.
- Caractéristique supplémentaire pour la création de rapports sur la version du micrologiciel PSU (unité d'alimentation secteur) sur la page **Informations sur les blocs d'alimentation**.

- Conformément à la recommandation de Citrix, la prise en charge du serveur Web depuis le nœud géré Xenserver 6.0 est dépréciée pour ne pas charger Dom0 avec des options de ressources restreintes. Utilisez le serveur Web de Server Administrator qui est installé sur un système séparé pour gérer XenServer 6.0.
- Attributs de réseau de basculement ajoutés à iDRAC (Dell Remote Access Controller) 7
- Les fonctionnalités de surveillance de l'alimentation sont désactivées si la licence Enterprise ne se trouve pas dans iDRAC7
- Le système BIOS et le mot de passe de configuration peuvent être définis à l'aide de l'interface GUI (interface utilisateur graphique) ou de l'interface CLI (Interface de ligne de commande). Dans la CLI, vous devez fournir le mot de passe pour chaque configuration d'attribut de configuration du BIOS. Vous devez également saisir le mot de passe de configuration lorsque vous utilisez la GUI dans le but de modifier les attributs de configuration du BIOS.
- Server Administrator exécute l'environnement JRE (Java Run Time Environment) 1.6 Mise à jour 30 (1.60_30) pour récupérer les correctifs de sécurité Java les plus récents.
- Le champ **Ports iDRAC** fait partie des propriétés d'accès à distance (iDRAC7) et est ajouté sur la page **Informations sur l'accès à distance**. Il indique la présence ou non d'adaptateur d'activation de gestion avancée (AMEA).
- Prise en charge dépréciée de Mozilla Firefox 3.6
- Prise en charge dépréciée des systèmes *xx8x*

Pour une liste des prises en charge supplémentaires et dépréciées des plateformes, des systèmes d'exploitation et des navigateurs, référez-vous à la Matrice de prise en charge logicielle des systèmes Dell de version 7.0 à l'adresse **support.dell.com/manuals→ Logiciel→ Gestion des systèmes→ Versions Dell OpenManage**.

Consultez l'aide en ligne contextuelle de Server Administrator pour obtenir des informations supplémentaires sur les nouvelles fonctionnalités introduites dans cette version.

Disponibilité de Systems Management Standards

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

- Protocole HTTPS (HyperText Transfer Protocol Secure)
- Modèle commun d'informations (CIM)
- Simple Network Management Protocol (SNMP)

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

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

Pour des informations sur les problèmes de sécurité SNMP, consultez le fichier « **Lisez-moi** » de Dell OpenManage Server Administrator (empaqueté avec l'application Server Administrator) ou consultez le site Web de support Dell à l'adresse **support.dell.com/manuals**. Vous devez appliquer les mises à jour depuis les agents de référence SNMP de votre système d'exploitation pour faire en sorte que les sous-agents SNMP de Dell soient sécurisés.

Disponibilité sur les systèmes d'exploitation pris en charge

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

Server Administrator offre un gain considérable de sécurité à ces normes Systems Management. Toutes les opérations de définition d'attributs (par exemple, la modification de la valeur d'un numéro d'inventaire) doivent être effectuées avec Dell OpenManage IT Assistant alors que la connexion a été établie avec l'autorité requise.

Tableau 1-1 indique les normes Systems Management disponibles pour chaque système d'exploitation pris en charge.

Tableau 1-1. Disponibilité de Systems Management Standards

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

Page d'accueil de Server Administrator

La page d'accueil de **Server Administrator** propose des tâches de gestion des systèmes, avec un navigateur Web, faciles à configurer et à utiliser depuis le système géré ou un hôte distant via un réseau local (LAN), un service de numérotation ou un réseau sans fil. Lorsque Dell Systems Management Server Administrator Connection Service (DSM SA Connection Service) est installé et configuré sur le système géré, vous pouvez exécuter des fonctions de gestion à distance depuis tout système disposant d'un navigateur et d'une connexion Web pris en charge. La page d'accueil de **Server Administrator** fournit également une aide en ligne contextuelle étendue.

Autres documents utiles

En plus de ce manuel, les manuels suivants sont disponibles sur **support.dell.com/manuals**. Sur la page **Manuels**, cliquez sur **Logiciels→ Systems Management**. Cliquez sur le lien du produit approprié sur le côté droit pour accéder aux documents.

- La *matrice de prise en charge logicielle des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- Le *Guide d'installation de Dell OpenManage Server Administrator* contient des instructions qui vous aideront à installer Dell OpenManage Server Administrator.
- Le *Guide d'installation du logiciel de la station de gestion Dell OpenManage* contient des instructions qui vous aideront à installer le logiciel de la station de gestion Dell OpenManage.
- Le *Guide de référence SNMP de Dell OpenManage Server Administrator* fournit des informations sur la base d'informations de gestion (MIB) du protocole SNMP (Simple Network Management Protocol - protocole de gestion de réseau simple).
- Le *Guide de référence CIM de Dell OpenManage Server Administrator* répertorie le fournisseur du modèle commun d'informations (CIM), une extension du fichier de format d'objet de gestion standard (MOF).

- Le *Guide de référence des messages de Dell OpenManage Server Administrator* répertorie les messages qui s'affichent dans votre journal des alertes de la page d'accueil de **Server Administrator** ou sur le visualiseur d'événements de votre système d'exploitation.
- Le *Guide d'utilisation de l'interface de ligne de commande Dell OpenManage* décrit la totalité de l'interface de ligne de commande.
- Le *Guide d'utilisation d'Integrated Dell Remote Access Controller* fournit des informations détaillées sur la configuration et l'utilisation du contrôleur iDRAC.
- Le Guide d'utilisation de *Dell Chassis Management Controller* fournit des informations détaillées sur l'installation, la configuration et l'utilisation du contrôleur CMC.
- Le *Guide d'utilisation de Dell Online Diagnostics* fournit des informations complètes sur l'installation et l'utilisation de Online Diagnostics sur votre système.
- Le *Guide d'utilisation de Dell OpenManage Baseboard Management Controller Utilities* fournit des informations supplémentaires sur l'utilisation de Server Administrator pour configurer et gérer le contrôleur BMC de votre système.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator Storage Management* est un guide de référence complet pour la configuration et la gestion du stockage local et distant connecté à un système.
- Le *Guide d'utilisation de l'utilitaire Racadm de Dell Remote Access Controller* fournit des informations sur l'utilisation de l'utilitaire de ligne de commande racadm.
- Le *Guide d'utilisation de Dell Remote Access Controller 5* fournit des informations complètes sur l'installation et la configuration d'un contrôleur DRAC 5 et son utilisation pour accéder à distance à un système ne fonctionnant pas.
- Le *Guide d'utilisation des progiciels Dell Update Packages* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Packages dans le cadre de votre stratégie de mise à jour du système.

- Consultez le *Guide d'utilisation de Dell OpenManage Server Update Utility* pour plus d'informations sur la manière d'obtenir et d'utiliser Server Update Utility (SUU) pour mettre à jour vos systèmes Dell ou pour afficher les mises à jour disponibles pour n'importe quel système répertorié dans l'espace de stockage.
- Le *Guide d'utilisation de Dell Management Console* contient des informations sur l'installation, la configuration et l'utilisation de Dell Management Console.
- Le *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 *Guide d'utilisation de Dell License Manager* fournit des informations sur la gestion des licences de serveur de composant pour serveurs Dell yx2x.
- Le *Glossaire* pour des informations sur la terminologie utilisée dans le présent document.

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 disponibles pour vous assister. Pour des informations supplémentaires sur ces outils d'aide, consultez la section « Obtention d'aide » du *Manuel du propriétaire de matériel* de votre système.

De plus, le programme Dell Enterprise Training and Certification est disponible ; consultez **dell.com/training** pour des informations supplémentaires. Ce service n'est disponible que dans certains pays.

2

Configuration et administration

Gestion de la sécurité

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

Contrôle de l'accès basé sur les rôles

Le RBAC gère la sécurité en déterminant les opérations pouvant être exécutées par des personnes avec des rôles particuliers. Chaque utilisateur se voit attribuer un ou plusieurs rôles et chaque rôle est accompagné d'un ou plusieurs privilèges d'utilisateur octroyés aux utilisateurs jouant ce rôle spécifique. Avec le RBAC, l'administration de la sécurité ressemble étroitement à la structure d'une organisation.

Privilèges d'utilisateur

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

- Les *utilisateurs* peuvent afficher la plupart des informations.
- Les *utilisateurs privilégiés* peuvent définir les valeurs des seuils d'avertissement et configurer les actions d'alerte qui doivent être effectuées lorsqu'un événement d'avertissement ou de panne se produit.
- Les *administrateurs* peuvent configurer et effectuer des actions d'arrêt, configurer des actions de restauration automatique au cas où le système d'exploitation d'un système ne répondrait pas et effacer les journaux de matériel, d'événements et de commandes. Les *administrateurs* peuvent également configurer le système pour envoyer des e-mails.
- *Les administrateurs élevés* peuvent afficher et gérer les informations.

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*. Voir Tableau 2-1.

Tableau 2-1. Privilèges d'utilisateur

Privilèges d'utilisateur	Type d'accès	
	Afficher	**Gérer**
Utilisateur	Oui	Non
Utilisateur privilégié	Oui	Oui
Administrateur	Oui	Oui
Administrateur élevé (Linux uniquement)	Oui	Oui

Niveaux de privilèges pour accéder aux services de Server Administrator

Le Tableau 2-2 récapitule les utilisateurs ayant des privilèges d'accès et de gestion concernant les services de Server Administrator.

Tableau 2-2. Niveaux de privilèges d'utilisateur de Server Administrator

Service	Niveau de privilège d'utilisateur requis	
	Afficher	**Gérer**
Instrumentation	U, P, A, EA	P, A, EA
Accès à distance	U, P, A, EA	A, EA
Storage Management (Gestion du stockage)	U, P, A, EA	A, EA

Tableau 2-3 définit les abréviations des niveaux de privilèges d'utilisateur utilisées dans Tableau 2-2.

Tableau 2-3. Légende des niveaux de privilèges d'utilisateur de Server Administrator

U	Utilisateur
P	Utilisateur privilégié
A	Administrateur
EA	Administrateur élevé

Authentification

Le schéma d'authentification de Server Administrator vérifie que les types d'accès corrects sont attribués aux privilèges d'utilisateur corrects. En outre, lorsque l'interface de ligne de commande (CLI) est invoquée, le schéma d'authentification de Server Administrator valide le contexte dans lequel le processus en cours s'exécute. Ce schéma d'authentification permet de s'assurer que toutes les fonctions de Server Administrator, qu'elles soient accessibles via la page d'accueil de **Server Administrator** ou la CLI, sont correctement authentifiées.

Authentification de Microsoft Windows

Pour les systèmes d'exploitation Microsoft Windows pris en charge, l'authentification de Server Administrator utilise l'authentification Windows intégrée (anciennement NTLM). Ce système d'authentification permet l'incorporation de la sécurité de Server Administrator à un schéma global de sécurité pour votre réseau.

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

Les diverses méthodes d'authentification de Server Administrator pour les systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge s'articulent autour de la bibliothèque des modules d'authentification enfichables (PAM). Les utilisateurs peuvent ouvrir une session sur Server Administrator localement ou à distance à l'aide de différents protocoles de gestion de comptes, tels que LDAP, NIS, Kerberos et Winbind.

Authentification de VMware ESX Server 4.X

VMware ESX Server utilise la structure des modules PAM (Pluggable Authentication Modules - Modules d'authentification enfichables) pour authentifier les utilisateurs qui accèdent à l'hôte ESX Server. La configuration PAM pour les services VMware se trouve dans **/etc/pam.d/vmware-authd** qui stocke les chemins d'accès aux modules d'authentification.

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

REMARQUE : Sur les systèmes fonctionnant sous le système d'exploitation VMware ESX Server 4.x, tous les utilisateurs doivent être dotés de droits d'administrateur pour pouvoir ouvrir une session Server Administrator. Pour obtenir des informations sur l'attribution de rôles, consultez la documentation VMware.

Authentification de VMware ESXi Server 5.X P1

ESXi Server authentifie les utilisateurs qui accèdent aux hôtes ESXi à l'aide du client vSphere/VI Client ou du kit de développement logiciel (SDK). L'installation par défaut de ESXi utilise une base de données de mots de passe locale pour l'authentification. Les transactions d'authentification de ESXi avec Server Administrator sont également des interactions directes avec le processus **vmware-hostd**. Pour que l'authentification s'exécute le mieux possible pour votre site, effectuez les tâches de base suivantes : définir les utilisateurs, les groupes, les autorisations et les rôles, définir les attributs utilisateurs, ajouter vos propres certifications et déterminer si vous voulez utiliser SSL.

REMARQUE : Sur les systèmes fonctionnant sous le système d'exploitation VMware ESXi Server 5.0 P1, tous les utilisateurs doivent être dotés de droits d'administrateur pour pouvoir ouvrir une session Server Administrator. Pour obtenir des informations sur l'attribution de rôles, consultez la documentation VMware.

Cryptage

L'accès à Server Administrator est assuré par une connexion HTTPS sécurisée qui utilise la technologie Secure Socket Layer (SSL) pour sécuriser et protéger l'identité du système géré. L'extension Java Secure Socket Extension (JSSE) est utilisée par les systèmes d'exploitation Microsoft Windows, Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge pour protéger les références de l'utilisateur et autres données sensibles qui sont transmises par la connexion du socket lorsque l'utilisateur accède à la page d'accueil de **Server Administrator**.

Attribution des privilèges d'utilisateur

Pour assurer la sécurité des composants système critiques, vous devez attribuer correctement les privilèges utilisateur à tous les utilisateurs des logiciels Dell OpenManage avant d'installer ceux-ci. Les nouveaux utilisateurs peuvent ouvrir une session sur le logiciel Dell OpenManage avec les 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 chaque compte d'utilisateur qui a accès au logiciel Dell OpenManage. Les utilisateurs sans mot de passe attribué ne peuvent pas se connecter au logiciel Dell OpenManage sur un système exécutant Windows Server 2003 en raison de la conception du système d'exploitation.

PRÉCAUTION : Désactivez les comptes d'invités sur les systèmes d'exploitation Windows pris en charge afin de protéger l'accès à vos composants système critiques. Il serait utile de renommer les comptes invités de façon à empêcher les sripts distants d'activer des comptes à l'aide de noms d'invités par défaut.

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

REMARQUE : Ajoutez de nouveaux utilisateurs au système d'exploitation si vous voulez ajouter des utilisateurs au logiciel OpenManage. Vous n'avez pas besoin de créer de nouveaux utilisateurs depuis le logiciel OpenManage.

Ajout d'utilisateurs à un domaine sur un système d'exploitation Windows

REMARQUE : Vous devez avoir installé Microsoft Active Directory sur votre système pour pouvoir effectuer les procédures suivantes. Voir « Utilisation de l'ouverture de session Active Directory », à la page 50 pour plus d'informations sur l'utilisation d'Active Directory.

1. Naviguez vers **Panneau de configuration**→ **Outils d'administration**→ **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, cliquez-droite 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 **Suivant**.
4. Cliquez sur **Suivant** puis sur **Terminer**.
5. Double-cliquez sur l'icône représentant l'utilisateur que vous venez de créer.
6. Cliquez sur l'onglet **Membre de**.
7. Cliquez sur **Ajouter**.
8. Sélectionnez le groupe approprié et cliquez sur **Ajouter**.
9. Cliquez sur **OK**, puis cliquez de nouveau sur **OK**.

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

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

Les privilèges d'accès d'administrateur sont attribués à l'utilisateur connecté en tant que `root`. Pour créer des utilisateurs ayant des privilèges d'utilisateur et d'utilisateur privilégié, effectuez les étapes suivantes.

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

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

Création d'utilisateurs

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

Création d'utilisateurs avec des privilèges d'utilisateur

1. Exécutez la commande suivante à partir de la ligne de commande :

   `useradd -d <répertoire de base> -g <groupe> <nom d'utilisateur>`

   où `<groupe>` n'est *pas* `root`.

   REMARQUE : Si `<groupe>` 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 à partir de la ligne de commande :

`useradd -d <répertoire de base> -g root <nom d'utilisateur>`

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 : Connectez-vous en tant qu'utilisateur `root` ou utilisateur équivalent pour effectuer ces procédures.

1 Ouvrez le fichier **omarolemap** qui se trouve dans **/opt/dell/srvadmin/etc/omarolemap**.

2 Ajoutez la ligne suivante au fichier :

`<Nom_d'utilisateur>[Tab]<Nom_d'hôte>[Tab]<Droits>`

Le Tableau 2-4 répertorie les légendes concernant l'ajout de la définition du rôle au fichier *omarolemap*.

Tableau 2-4. Légendes concernant l'ajout de la définition du rôle dans OpenManage Server Administrator

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

Le Tableau 2-5 répertorie les exemples concernant l'ajout de la définition du rôle au fichier *omarolemap*.

Tableau 2-5. Exemples concernant l'ajout de la définition du rôle dans OpenManage Server Administrator

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

3 Enregistrez les modifications et fermez le fichier.

Meilleures pratiques lors de l'utilisation du fichier omarolemap

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

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

root	*	Administrateur
+root	*	Utilisateur privilégié
*	*	Utilisateur

- Ne modifiez pas les permissions ou le format du fichier **omarolemap**.
- N'utilisez pas l'adresse de retour de boucle pour *<Nom_d'hôte>* par exemple : hôte local ou 127.0.0.1.
- Lorsque les services de connexion ont été redémarrés et que les modifications ne sont pas effectives pour le fichier **omarolemap**, consultez le journal des commandes pour prendre connaissance des erreurs.
- Lorsque le fichier **omarolemap** est copié d'un ordinateur à un autre, les permissions et les entrées du fichier doivent être revérifiées.
- Ajoutez le préfixe + au *Nom du groupe*.

- Server Administrator utilise les privilèges utilisateur par défaut du système d'exploitation si :
  - un utilisateur est dégradé dans le fichier **omarolemap**
  - il existe des saisies en double de noms d'utilisateurs et de groupes d'utilisateurs présentant en outre le même *<Hôte_Nom>*
- *Espace* peut également être utilisé comme délimiteur pour les colonnes au lieu de [Tab].

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

Pour ajouter un utilisateur au tableau répertoriant les utilisateurs :

1. Connectez-vous à l'hôte via vSphere Client.
2. Cliquez sur l'onglet **Utilisateurs et Groupes**, puis cliquez sur **Utilisateurs**.
3. Avec le bouton droit de la souris, cliquez n'importe où dans le tableau Utilisateurs, puis cliquez sur **Ajouter** pour ouvrir la boîte de dialogue **Ajouter un nouvel utilisateur**.
4. Entrez un nom d'accès, un nom d'utilisateur, une réf. utilisateur numérique (IUD) et un mot de passe ; la saisie du nom d'utilisateur et de la réf. utilisateur est facultative. Si vous ne spécifiez pas la réf. utilisateur, le vSphere Client attribue la réf. utilisateur disponible suivante.
5. Pour permettre à un utilisateur d'accéder à l'hôte ESX/ESXi via un environnement de commande, sélectionnez **Autoriser cet utilisateur à accéder à l'environnement**. Les utilisateurs qui accèdent à l'hôte uniquement via vSphere Client n'ont pas besoin d'avoir accès à l'environnement.
6. Pour ajouter un utilisateur à un groupe, sélectionnez le nom du groupe dans le menu déroulant **Groupe** et cliquez sur **Ajouter**.
7. Cliquez sur **OK**.

Désactivation de comptes d'invités et anonymes sur un système d'exploitation Windows pris en charge

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

1. Ouvrez la fenêtre **Gestion de l'ordinateur**.
2. Dans l'arborescence de la console, développez **Utilisateurs et groupes locaux** et cliquez sur **Utilisateurs**.
3. Double-cliquez sur le compte d'utilisateur dénommé **Invité** ou **système_IUSR** pour afficher les propriétés de ces utilisateurs, ou cliquez-droite sur le compte d'utilisateur dénommé **Invité** ou **système_IUSR**, puis choisissez **Propriétés**.
4. Sélectionnez **Le compte est désactivé** et cliquez sur **OK**.

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

Configuration de l'agent SNMP

Server Administrator prend en charge la norme SNMP (Simple Network Management Protocol - Norme de gestion de systèmes de réseau simple) sur tous les systèmes d'exploitation pris en charge. La prise en charge SNMP peut être installée ou non installée selon votre système d'exploitation et la manière dont le système d'exploitation a été installé. Dans la plupart des cas, SNMP est installé lors de l'installation de votre système d'exploitation. L'installation d'une norme de protocole de gestion de systèmes prise en charge telle que SNMP est requise avant de pouvoir installer Server Administrator.

Vous pouvez configurer l'agent SNMP pour modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à une station de gestion. Pour configurer votre agent SNMP en vue d'une interaction adéquate avec des applications de gestion comme Dell OpenManage IT Assistant, effectuez les procédures décrites dans les sections suivantes.

REMARQUE : La configuration par défaut de l'agent SNMP comprend généralement un nom de communauté SNMP tel que **public**. Pour des raisons de sécurité, modifiez les noms de communauté SNMP par défaut. Pour des informations sur la manière de changer les noms de communauté SNMP, reportez-vous à la section correspondante ci-dessous.

REMARQUE : Les opérations set SNMP sont désactivées par défaut dans Server Administrator version 5.2 ou ultérieure. Server Administrator prend en charge l'activation et la désactivation des opérations set SNMP dans Server Administrator. Vous pouvez utiliser la page **Configuration SNMP de Server Administrator** sous **Préférences** ou l'interface de ligne de commande (CLI) de Server Administrator pour activer ou désactiver les opérations set SNMP dans Server Administrator. Pour des informations supplémentaires sur la CLI de Server Administrator, consultez le *Guide d'utilisation de l'interface de ligne de commande de Dell OpenManage Server Administrator*.

REMARQUE : Pour qu'IT Assistant puisse récupérer les informations de gestion d'un système exécutant Server Administrator, le nom de communauté utilisé par IT Assistant doit correspondre au nom de communauté du système exécutant Server Administrator. Pour qu'IT Assistant puisse modifier des informations ou effectuer des actions sur un système exécutant Server Administrator, le nom de communauté utilisé par IT Assistant doit correspondre au nom de communauté autorisant les opérations set sur le système exécutant Server Administrator. Pour qu'IT Assistant puisse recevoir des interruptions (notifications d'événements asynchrones) d'un système exécutant Server Administrator, le système qui exécute Server Administrator doit être configuré pour pouvoir envoyer des interruptions au système qui exécute IT Assistant.

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

- « Configuration de l'agent SNMP pour les systèmes fonctionnant sous un système d'exploitation Windows pris en charge » à la page 29.
- « Configuration de l'agent SNMP sur les systèmes fonctionnant sous un système d'exploitation Red Hat Enterprise Linux pris en charge » à la page 32.
- « Configuration de l'agent SNMP sur les systèmes fonctionnant sous des systèmes d'exploitation SUSE Linux Enterprise Server pris en charge » à la page 36.
- « Configuration de l'agent SNMP sur des systèmes fonctionnant sous les systèmes d'exploitation VMware ESX 4.X pris en charge sur les bases d'informations de gestion Proxy VMware » à la page 39.
- « Configuration de l'agent SNMP sur des systèmes exécutant les systèmes d'exploitation VMware ESXi 4.X et ESXi 5.X pris en charge » à la page 41.

Configuration de l'agent SNMP pour les systèmes fonctionnant sous un système d'exploitation Windows pris en charge

Server Administrator utilise les services SNMP fournis par l'agent SNMP de Windows. Vous pouvez configurer l'agent SNMP pour modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à une station de gestion. Pour configurer votre agent SNMP pour une interaction adéquate avec des applications de gestion comme IT Assistant, procédez comme décrit dans les sections suivantes.

REMARQUE : Consultez la documentation de votre système d'exploitation pour obtenir des détails supplémentaires sur la configuration SNMP.

Activation de l'accès SNMP par les hôtes distants

Par défaut, Windows Server 2003 n'accepte pas les paquets SNMP provenant d'hôtes distants. Pour les systèmes exécutant Windows Server 2003, vous devez configurer le service SNMP de façon à ce qu'il accepte les paquets SNMP provenant d'hôtes distants si vous voulez gérer le système en utilisant des applications de gestion SNMP provenant d'hôtes distants.

Pour activer un système exécutant le système d'exploitation Windows Server 2003 afin de recevoir des paquets SNMP provenant d'un hôte distant, effectuez les étapes suivantes :

1. Ouvrez la fenêtre **Gestion de l'ordinateur**.
2. Développez l'icône **Gestion de l'ordinateur** dans la fenêtre, au besoin.
3. Développez l'icône **Services et applications** et cliquez sur **Services**.
4. Faites défiler la liste des services jusqu'à ce que vous trouviez **Service SNMP**, cliquez-droite sur **Service SNMP**, puis cliquez sur **Propriétés**.

   La fenêtre **Propriétés du service SNMP** apparaît.
5. Cliquez sur l'onglet **Sécurité**.
6. Sélectionnez **Accepter les paquets SNMP provenant de n'importe quel hôte** ou ajoutez l'hôte distant à la liste **Accepter les paquets SNMP provenant de ces hôtes**.

Modification du nom de communauté SNMP

La configuration des noms de communauté SNMP détermine les systèmes qui peuvent gérer votre système via SNMP. Le nom de communauté SNMP utilisé par les applications de gestion doit correspondre au nom de communauté SNMP configuré sur le système Server Administrator pour que les applications de gestion puissent récupérer les informations de gestion depuis Server Administrator.

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

   La fenêtre **Propriétés du service SNMP** apparaît.
5. Cliquez sur l'onglet **Sécurité** pour ajouter ou modifier un nom de communauté.

   Pour ajouter un nom de communauté :

   a. Cliquez sur **Ajouter** sous la liste **Noms de communs acceptés**.

      La fenêtre **Configuration du service SNMP** apparaît.

   b. Tapez 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 **Ajouter**.

      La fenêtre **Propriétés du service SNMP** apparaît.

   Pour modifier un nom de communauté :

   a. Sélectionnez un nom de communauté dans la liste **Noms de communauté acceptés** et cliquez sur **Modifier**.

      La fenêtre **Configuration du service SNMP** apparaît.

   b. Faites toutes les modifications nécessaires au nom de communauté du système qui est capable de gérer votre système dans la zone de texte **Nom de communauté** et cliquez sur **OK**.

      La fenêtre **Propriétés du service SNMP** apparaît**.**
6. Cliquez sur **OK** pour enregistrer les changements.

Activation des opérations set SNMP

Les opérations set SNMP doivent être activées sur le système exécutant Server Administrator pour pouvoir changer les attributs de Server Administrator avec IT Assistant.

1. Ouvrez la fenêtre **Gestion de l'ordinateur**.
2. Développez l'icône **Gestion de l'ordinateur** dans la fenêtre, au besoin.
3. Développez l'icône **Services et applications** et cliquez sur **Services**.
4. Faites défiler la liste des services jusqu'à ce que vous trouviez **Service SNMP**, cliquez-droite sur **Service SNMP**, puis cliquez sur **Propriétés**.

   La fenêtre **Propriétés du service SNMP** apparaît.
5. Cliquez sur l'onglet **Sécurité** pour modifier les droits d'accès d'une communauté.
6. Sélectionnez un nom de communauté dans la liste **Noms de communauté acceptés** et cliquez sur **Modifier**.

   La fenêtre **Configuration du service SNMP** apparaît.
7. Définissez les **droits de communauté** sur **LECTURE ÉCRITURE** ou **LECTURE CRÉATION**, puis cliquez sur **OK**.

   La fenêtre **Propriétés du service SNMP** apparaît.
8. Cliquez sur **OK** pour enregistrer les changements.

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 Server Administrator pour que les interruptions SNMP soient envoyées à une station de gestion.

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

La fenêtre **Propriétés du service SNMP** apparaît.

5 Cliquez sur l'onglet **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 **Nom de la communauté** et cliquez sur **Ajouter à la liste**, à côté de la boîte **Nom de la communauté**.

   b Pour ajouter une destination d'interruption pour une communauté d'interruptions, sélectionnez le nom de communauté dans la boîte déroulante **Nom de la communauté** et cliquez sur **Ajouter** sous la boîte **Destinations d'interruption**.

      La fenêtre **Configuration du service SNMP** apparaît.

   c Tapez la destination de l'interruption et cliquez sur **Ajouter**.

      La fenêtre **Propriétés du service SNMP** apparaît.

6 Cliquez sur **OK** pour enregistrer les changements.

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

Server Administrator utilise les services SNMP fournis par l'agent SNMP ***net-snmp***. Vous pouvez configurer l'agent SNMP de sorte à modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à une station de gestion. Pour configurer votre agent SNMP pour une interaction adéquate avec des applications de gestion comme IT Assistant, effectuez les procédures décrites dans les sections suivantes.

REMARQUE : Consultez la documentation de votre système d'exploitation pour obtenir des détails supplémentaires sur la configuration SNMP.

Configuration du contrôle d'accès de l'agent SNMP

La branche de la base d'informations de gestion (MIB) implémentée par Server Administrator est identifiée par l'OID 1.3.6.1.4.1.674. Les applications de gestion doivent avoir accès à cette branche de l'arborescence MIB pour pouvoir gérer les systèmes exécutant Server Administrator.

Pour les systèmes d'exploitation Red Hat Enterprise Linux et VMware ESXi 4.0, la configuration de l'agent SNMP par défaut octroie un accès en lecture seule à la branche système MIB-II (identifiée par l'OID 1.3.6.1.2.1.1) de l'arborescence MIB pour la communauté type « public ». Cette configuration

ne permet pas aux applications de gestion de récupérer ou de modifier les informations de gestion de Server Administrator ou d'autres systèmes hors de la branche *système* MIB-II.

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

Si Server Administrator détecte la configuration SNMP par défaut pendant l'installation, il tente de modifier la configuration de l'agent SNMP pour octroyer un accès en lecture seule à toute l'arborescence MIB pour la communauté « *public* ». Server Administrator modifie de deux façons le fichier de configuration de l'agent SNMP **/etc/snm, p/snmpd.conf** :

La première modification consiste à créer une vue de toute l'arborescence MIB en ajoutant la ligne suivante si elle n'existe pas :

```
view all included .1
```

La seconde modification consiste à modifier la ligne *d'accès* par défaut pour offrir un accès en lecture seule à toute l'arborescence MIB pour la communauté *public*. Server Administrator cherche la ligne suivante :

```
access notConfigGroup "" any noauth exact systemview
none none
```

Si Server Administrator trouve la ligne ci-dessus, il modifie la ligne de la manière suivante :

```
access notConfigGroup "" any noauth exact all none none
```

Ces modifications apportées à la configuration de l'agent SNMP par défaut offrent un accès en lecture seule à toute l'arborescence MIB pour la communauté *public*.

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.

Server Administrator SNMP communique avec l'agent SNMP selon le protocole de multiplexage SNMP (SMUX). Quand Server Administrator SNMP se connecte à l'agent SNMP, il envoie un identificateur d'objet à l'agent SNMP pour s'identifier comme un homologue SMUX. Étant donné que cet identificateur d'objet doit être configuré avec l'agent SNMP, Server Administrator ajoute la ligne suivante au fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) pendant l'installation si elle n'existe pas :

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Modification du nom de communauté SNMP

La configuration du nom de communauté SNMP détermine les systèmes qui peuvent gérer votre système via SNMP. Le nom de communauté SNMP utilisé par les applications de gestion doit correspondre au nom de communauté SNMP configuré sur le système Server Administrator pour que les applications de gestion puissent récupérer les 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, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) et procédez comme suit :

1. Trouvez la ligne :

   ```
   com2sec publicsec default public
   ```

   ou

   ```
   com2sec notConfigUser default public
   ```

2. Modifiez cette ligne en remplaçant `public` par le nouveau nom de communauté SNMP. Une fois modifiée, la nouvelle ligne est la suivante :

   ```
   com2sec publicsec default nom_de_communauté
   ```

   ou

   ```
   com2sec notConfigUser default nom_de_communauté
   ```

3. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant :

   ```
   service snmpd restart
   ```

Activation des opérations Set SNMP

Les opérations set SNMP doivent être activées sur le système exécutant Server Administrator pour pouvoir changer les attributs de Server Administrator avec IT Assistant.

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

1 Trouvez la ligne :

```
access publicgroup "" any noauth exact all none
none
```

ou

```
access notConfigGroup "" any noauth exact all none
none
```

2 Modifiez cette ligne en remplaçant la première valeur `none` (aucun) par `all` (tous). Une fois modifiée, la nouvelle ligne est la suivante :

```
access publicgroup "" any noauth exact all all
none
```

ou

```
access notConfigGroup "" any noauth exact all all
none
```

3 Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant :

```
service snmpd restart
```

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

Server Administrator génère des interruptions SNMP en réponse aux modifications de la condition des capteurs et d'autres paramètres surveillés. Vous devez configurer une ou plusieurs destinations d'interruption sur le système exécutant Server Administrator pour que les interruptions SNMP puissent être envoyées 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` *`adresse_IP nom_de_communauté`*

où *`adresse_IP`* est l'adresse IP de la station de gestion et *`nom_de_communauté`* 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 à partir d'hôtes distants, modifier le nom de communauté, activer les opérations Set et envoyer des interruptions à une station de gestion. Pour configurer votre agent SNMP pour une interaction adéquate avec des applications de gestion comme IT Assistant, effectuez les procédures décrites dans les sections suivantes.

REMARQUE : Consultez la documentation de votre système d'exploitation pour des détails supplémentaires sur la configuration SNMP.

Actions d'installation de Server Administrator SNMP

Server Administrator SNMP communique avec l'agent SNMP selon le protocole SMUX. Quand Server Administrator SNMP se connecte à l'agent SNMP, il envoie un identificateur d'objet à l'agent SNMP pour s'identifier comme un homologue SMUX. Étant donné que cet identificateur d'objet doit être configuré avec l'agent SNMP, Server Administrator ajoute la ligne suivante au fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) pendant l'installation, si elle n'existe pas encore :

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

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

La configuration de l'agent SNMP par défaut sur les systèmes d'exploitation SUSE Linux Enterprise Server donne un accès en lecture seule à l'ensemble de l'arborescence MIB pour la communauté *public* à partir de l'hôte local uniquement. Cette configuration n'autorise pas les applications de gestion SNMP comme IT Assistant à fonctionner sur d'autres hôtes afin de détecter et gérer correctement les systèmes Server Administrator. Si Server Administrator découvre cette configuration pendant l'installation, il journalise un message dans le fichier journal du système d'exploitation **/var/log/messages** pour indiquer que l'accès SNMP est restreint à l'hôte local. Vous devez configurer l'agent SNMP pour activer l'accès SNMP à partir d'hôtes distants si vous projetez de gérer le système en utilisant des applications de gestion SNMP depuis des 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 est la suivante :

   ```
   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 (/e**tc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Trouvez la ligne :

   ```
   rocommunity public 127.0.0.1
   ```

2. Modifiez cette ligne en supprimant 127.0.0.1. Une fois modifiée, la nouvelle ligne est la suivante :

   ```
   rocommunity public
   ```

3. 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 du nom de communauté SNMP détermine quelles stations de gestion peuvent gérer votre système par SNMP. Le nom de communauté SNMP utilisé par les applications de gestion doit correspondre au nom de

communauté SNMP configuré sur le système Server Administrator pour que les applications de gestion puissent récupérer les 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, 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 cette ligne en remplaçant `public` par le nouveau nom de communauté SNMP. Une fois modifiée, la nouvelle ligne est la suivante :

   ```
   rocommunity nom_de_communauté 127.0.0.1
   ```

3. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant :

   ```
   /etc/init.d/snmpd restart
   ```

Activation des opérations Set SNMP

Les opérations set SNMP doivent être activées sur le système exécutant Server Administrator pour pouvoir changer les attributs de Server Administrator avec IT Assistant. Pour activer l'arrêt à distance d'un système à partir d'IT Assistant, les opérations set SNMP doivent être activées.

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

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

1. Trouvez la ligne :

   ```
   rocommunity public 127.0.0.1
   ```

2. Modifiez cette ligne en remplaçant `rocommunity` par `rwcommunity`. Une fois modifiée, la nouvelle ligne est la suivante :

   ```
   rwcommunity public 127.0.0.1
   ```

3. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant :

```
/etc/init.d/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 la condition des capteurs et d'autres paramètres surveillés. Vous devez configurer une ou plusieurs destinations d'interruption sur le système exécutant Server Administrator pour que les interruptions SNMP puissent être envoyées 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` *`adresse_IP nom_de_communauté`*

   où `adresse_IP` est l'adresse IP de la station de gestion et `nom_de_communauté` est le nom de la communauté SNMP.

2. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant :

   ```
   /etc/init.d/snmpd restart
   ```

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

Le serveur ESX 4.X peut être géré via un seul port par défaut (162) à l'aide du protocole SNMP. Pour cela, `snmpd` est configuré pour utiliser le port 162 par défaut et `vmwarehostd` est configuré pour utiliser un port différent (inutilisé), par exemple, 167. Toutes les requêtes SNMP sur la branche des bases d'informations de gestion VMWare sont alors réacheminées vers ***vmware-hostd*** via la fonctionnalité proxy du démon ***snmpd***.

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

Pour configurer l'agent SNMP :

1. Modifiez manuellement le fichier de configuration SNMP de VMWare **/etc/vmware/snmp.xml** ou exécutez les commandes vicfg-snmp suivantes pour modifier les paramètres de la configuration SNMP. Ceci comprend le port d'écoute SNMP, la chaîne de communauté ainsi que l'adresse IP/le port de la cible d'interruption, et le nom de communauté d'interruption. Ensuite, activez le service SNMP VMWare.

   a. `vicfg-snmp --server <adr_IP_ESX> --username root --password <mot de passe> -c <nom de communauté> -p X -t <adr_IP_Destination>@162/<nom de communauté>`

   X représente un port non utilisé. Pour trouver un port inutilisé, analysez le fichier **/etc/services** pour l'attribution de port pour des services système définis. D'autre part, pour vous assurer que le port sélectionné n'est pas utilisé par une application ou un service quelconque, exécutez la commande suivante sur le serveur ESX : `netstat –a command`

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

   b. Pour activer le service SNMP VMWare, exécutez la commande suivante :

```
vicfg-snmp.pl --server <adr_IP_ESX> --username
root --password <mot de passe>

-E
```

   c. Pour afficher les paramètres de configuration, exécutez la commande suivante :

```
vicfg-snmp.pl --server <adr_IP_ESX> --username
root --password <mot de passe>

-s
```

   Une fois les modifications effectuées, le fichier de configuration se présente comme suit :

```
<?xml version="1.0">

<config>

<paramètres_snmp>
```

```
<activer>true</activer>

<communautés>public</communautés>

<cibles>143.166.152.248@162/public</cibles>

<port>167</port>

<paramètres_snmp>

<config>
```

2 Arrêtez le service SNMP s'il est déjà en cours d'exécution sur votre système en entrant la commande suivante :

```
service snmpd stop
```

3 Ajoutez la ligne suivante à la fin du fichier **/etc/snmp/snmp.conf** :

```
proxy -v 1 -c public udp:127.0.0.1:
X .1.3.6.1.4.1.6876
```

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

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

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

5 Redémarrez le service mgmt-vmware en utilisant la commande suivante :

```
service mgmt-vmware restart
```

6 Redémarrez le service snmpd en utilisant la commande suivante :

```
service snmpd start
```

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

7 Exécutez la commande suivante afin que le démon snmpd démarre lors de chaque redémarrage :

```
Chkconfig snmpd on
```

8 Exécutez la commande suivante pour garantir que les ports SNMP sont ouverts avant d'envoyer les interruptions à la station de gestion.

```
esxcfg-firewall -e snmpd
```

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

Server Administrator prend en charge les interruptions SNMP sur les systèmes VMware ESXi 4.X et ESXi 5.X. Si une licence autonome est uniquement présente, la configuration SNMP échoue sur les systèmes d'exploitation VMware ESXi. Server Administrator ne prend pas en charge les opérations Get et Set SNMP sur VMWare ESXi 4.X et ESXi 5.x car la prise en charge SNMP requise est non disponible. L'interface de ligne de commande (CLI) VMware vSphere est utilisée pour configurer un système qui exécute VMware ESXi 4.X et ESXi 5.x pour envoyer les interruptions SNMP vers une station de gestion.

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

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

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

Pour configurer votre système ESXi qui exécute Server Administrator pour qu'il puisse envoyer des interruptions à une station de gestion, effectuez les étapes suivantes :

1. Installez la CLI VMware vSphere.
2. Ouvrez une invite de commande sur le système où la CLI VMware vSphere est installée.
3. Placez-vous dans le répertoire dans lequel la CLI VMware vSphere est installée. Sur Linux, l'emplacement par défaut est **/usr/bin**. Sur Windows, l'emplacement par défaut 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, <mot_de_passe> correspond au mot de passe de l'utilisateur 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 qu'il soit 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 sélectionnez une sécurité par pare-feu lorsque vous installez Red Hat Enterprise Linux/SUSE Linux, le port SNMP de toutes les interfaces réseau externes est fermé par défaut. Pour que des applications de gestion SNMP, comme IT Assistant, puissent découvrir et extraire des informations de Server Administrator, le port SNMP doit être ouvert sur au moins l'une des interfaces réseau externes. Si Server Administrator détecte que le port SNMP n'est pas ouvert dans le pare-feu des interfaces réseau externes, Server Administrator affiche un message d'avertissement et journalise un message dans le journal du système.

Vous pouvez ouvrir le port SNMP en désactivant le pare-feu, en ouvrant toute une interface réseau externe dans le pare-feu ou en ouvrant le port SNMP pour au moins une interface réseau externe dans le pare-feu. Vous pouvez effectuer cette action avant ou après le démarrage de Server Administrator.

Pour ouvrir le port SNMP sur RHEL 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 **Choisir un outil** apparaît.

2. Sélectionnez **Configuration du pare-feu** avec la flèche vers le bas et appuyez sur <Entrée>.

   L'écran **Configuration du pare-feu** apparaît.

3. Appuyez sur <Tab> pour sélectionner **Niveau de sécurité**, puis sur la barre d'espace pour sélectionner le niveau de sécurité de votre choix. Le Niveau de sécurité sélectionné est indiqué par un astérisque.

   REMARQUE : Appuyez sur <F1> pour obtenir des informations supplémentaires sur les niveaux de sécurité du pare-feu. Le numéro de port SNMP par défaut est **161**. Si vous utilisez l'interface utilisateur graphique du système X Window, le fait d'appuyer sur <F1> risque de ne pas fournir d'informations sur les niveaux de sécurité du pare-feu sur les versions les plus récentes de Red Hat Enterprise Linux.

   a. Pour désactiver le pare-feu, sélectionnez **Pas de pare-feu** ou **Désactivé** et passez à étape 7.

   b. Pour ouvrir toute l'interface réseau ou le port SNMP, sélectionnez **Élevé, Moyen** ou **Activé** et passez à étape 4.

4. Appuyez sur <Tab> pour accéder à **Personnaliser** puis sur <Entrée>.

   L'écran **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 une interface réseau, appuyez sur <Tab> pour sélectionner un des périphériques approuvés et appuyez sur la barre d'espace. Un astérisque dans la boîte à gauche du nom du périphérique indique que toute l'interface est ouverte.

   b. Pour ouvrir le port SNMP sur toutes les interfaces réseau, appuyez sur **<Tab>** pour sélectionner **Autres ports** et tapez `snmp:udp`.

6 Appuyez sur **<Tab>** pour sélectionner **OK** puis sur **<Entrée>**.

L'écran **Configuration du pare-feu** apparaît.

7 Appuyez sur **<Tab>** pour sélectionner **OK** puis sur **<Entrée>**.

Le menu **Choisir un outil** apparaît.

8 Appuyez sur **<Tab>** pour sélectionner **Quitter** puis sur **<Entrée>**.

Pour ouvrir le port SNMP sur SUSE Linux Enterprise Server, procédez comme suit :

1 Configurez SuSEfirewall2 en exécutant cette commande sur une console
`a.# yast2 firewall`

2 Utilisez les touches fléchées pour naviguer vers **Services autorisés**.

3 Appuyez sur les touches **Alt+d** pour ouvrir la boîte de dialogue **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 les touches **Alt-O** et « **Alt-N** » pour passer à l'écran suivant.

7 Appuyez sur les touches **Alt-A** pour accepter et appliquer les modifications.

3

Utilisation de Server Administrator

Ouverture de votre session Server Administrator

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

L'écran**Server Administrator Log in** s'affiche. Le port par défaut de Dell OpenManage Server Administrator est 1311. Vous pouvez modifier le port, si nécessaire. Voir « Service de connexion Dell Systems Management Server Administration et configuration de la sécurité<Par défaut Font> » à la page 60 pour des instructions relatives à l'installation de vos préférences système.

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

Ouverture et fermeture de session

OpenManage Server Administrator fournit trois types d'ouverture de session. Parmi ceux-ci :

- Server Administrator sur le système local
- Server Administrator sur un système géré
- Central Web Server

Ouverture d'une session Server Administrator sur le système local

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

Cette option est disponible pour les serveurs exécutant XenServer 6.0

Pour ouvrir une session Server Administrator sur un système local :

1. Tapez votre **Nom d'utilisateur** et votre **Mot de passe** préattribués dans les champs appropriés de la fenêtre **Ouverture d'une session** 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 **Ouvrir une session Active Directory** pour ouvrir une session Microsoft Active Directory. Voir « Utilisation de l'ouverture de session Active Directory », à la page 50.

3 Cliquez sur **Envoyer**.

Pour mettre fin à votre session Server Administrator, cliquez sur le bouton **Fermer la session**, dans le coin supérieur droite 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 *Guide d'installation du logiciel OpenManage Management Station*.

Ouverture d'une session Server Administrator sur un système géré

Cette ouverture de session est disponible uniquement lorsque vous installez le composant Server Administrator Web Server. Pour ouvrir une session Server Administrator pour gérer un système distant :

Méthode 1

1 Double-cliquezsurl'icône **Dell OpenManage Server Administrator** sur votre bureau.

2 Tapez l'adresse IP du système géré, le nom du système ou le nom de domaine complet (FQDN).

REMARQUE : Si vous avez entré le nom du système ou le nom de domaine complet, l'hôte Dell OpenManage Server Administrator Web Server convertit le nom du système ou le nom de domaine complet en adresse IP du système géré. Vous pouvez également entrer le numéro de port du système géré. Par exemple, Nom d'hôte:Numéro de port ou Adresse IP:Numéro de port.
Si vous vous connectez à un nœud géré Citrix XenServer 6.0, utilisez le port 5986 au format Nom d'hôte:Numéro de port ou Adresse IP:Numéro de port.

3 Cochez la case **Ignorer les avertissements du certificat** si vous utilisez une connexion Intranet.

4 Cochez la case **Ouvrir une session Active Directory**. Cochez cette option pour ouvrir une session à l'aide de l'authentification Microsoft Active Directory. Ne cochez pas cette case si le logiciel Active Directory n'est pas utilisé pour contrôler l'accès à votre réseau. Voir « Utilisation de l'ouverture de session Active Directory », à la page 50.

5 Cliquez sur **Soumettre**.

Méthode 2

Ouvrez votre navigateur Web et tapez l'une des entrées suivantes dans le champ d'adresse et appuyez sur <Entrée> :

`https://nomd'hôte:1311`

où `nomd'hôte` est le nom attribué au système de nœud géré et `1311` le numéro de port par défaut

ou

`https://adresse IP:1311`

où `adresse IP` est l'adresse IP du système géré et `1311` le numéro de port par défaut Vous devez taper `https://` (et non `http://`) dans le champ d'adresse pour recevoir une réponse valide dans votre navigateur.

REMARQUE : Vous devez avoir des droits d'utilisateur préattribués pour pouvoir ouvrir une session sur Server Administrator. Voir « Configuration et administration », à la page 19 pour des instructions sur la configuration de nouveaux utilisateurs.

Ouverture d'une session Central Web Server

Cette ouverture de session est disponible uniquement lorsque vous installez le composant Server Administrator Web Server. Utilisez cette ouverture de session pour gérer OpenManage Server Administrator Central Web Server :

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

PRÉCAUTION : L'écran d'ouverture de session intègre la case à cocher Ignorer les avertissements du certificat. Soyez vigilant quant à l'utilisation de cette option. Il est recommandé de l'utiliser uniquement dans les environnements Intranet sécurisés.

2. Cliquez sur le lien **Gérer Web Server** qui se trouve dans le coin supérieur droit de l'écran.
3. Entrez les **Nom d'utilisateur**, **Mot de passe** et **Nom de domaine** (si vous accédez à Server Administrator à partir d'un domaine défini), puis cliquez sur **Soumettre**.
4. Cochez la case **Ouvrir une session Active Directory** pour ouvrir une session Microsoft Active Directory. Voir la « Utilisation de l'ouverture de session Active Directory », à la page 50.
5. Cliquez sur **Soumettre**.

Pour mettre fin à votre session Server Administrator, cliquez sur **Fermer la session** sur « Barre de navigation globale<Par défaut Font> ». Le bouton **Fermer la session** se trouve en haut à droite de chaque page d'accueil de **Server Administrator**.

REMARQUE : Lorsque vous lancez Server Administrator via Mozilla Firefox version 3.0 et 3.5 ou Microsoft Internet Explorer version 7.0 ou 8.0, une page d'avertissement intermédiaire affichant le problème inhérent au certificat de sécurité est susceptible d'apparaître. Pour garantir la sécurité du système, nous vous conseillons de générer un nouveau certificat X.509, de réutiliser un certificat X.509 existant ou d'importer un certificat racine ou une chaîne de certificat d'une autorité de certification (CA). Pour éviter que ces messages d'avertissement sur le certificat ne s'affichent, le certificat utilisé doit être émis par une CA fiable. Pour en savoir plus sur la gestion du certificat X.509, consultez « Gestion du certificat X.509 ».

Pour garantir la sécurité du système, nous vous recommandons d'importer un certificat racine ou une chaîne de certificat d'une autorité de certification (CA). Reportez-vous à la documentation de VMware pour plus de détails.

REMARQUE : Si l'autorité de certification du système géré est valide et que Server Administrator Web Server signale toujours une erreur de certificat non sécurisé, vous pouvez toujours définir l'autorité de certification du système géré comme étant digne de confiance en utilisant le fichier **certutil.exe**. Consultez la documentation de votre système d'exploitation pour obtenir des détails sur l'accès à ce fichier **.exe**. Sur les systèmes d'exploitation Windows pris en charge, vous pouvez également utiliser l'option de composant logiciel enfichable des certificats pour importer des certificats.

Utilisation de l'ouverture de session Active Directory

Vous devez cocher la case **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 fournir l'accès à Server Administrator, et d'ajouter et ou/contrôler des utilisateurs et des privilèges de Server Administrator aux utilisateurs existants dans votre logiciel Active Directory. Pour en savoir plus, voir « Utilisation de Microsoft Active Directory » du *Guide d'installation et de sécurité de Dell OpenManage*.

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 **Dell OpenManage Server Administrator** sur le bureau sans passer par la page d'ouverture de session.

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

Pour accéder à l'ordinateur local, il est nécessaire d'avoir un compte sur cet ordinateur avec des privilèges appropriés (utilisateur, utilisateur privilégié ou administrateur). Les autres utilisateurs sont authentifiés avec Microsoft Active Directory. Pour lancer Server Administrator en utilisant l'authentification par connexion directe au lieu de Microsoft Active Directory, ajoutez les paramètres suivants à :

```
authType=ntlm&application=[nom du plug-in]
```

where *nom du plug-in* = *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, ajoutez les paramètres suivants à :

```
authType=ntlm&application=[nom du plug-
in]&locallogin=true
```

Where *nom du plug-in* = *omsa*, *ita*, etc.

Par exemple :

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

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

Configuration des paramètres de sécurité sur des systèmes qui fonctionnent sous 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 fonctionne sous un système d'exploitation Microsoft Windows pris en charge.

Les paramètres de sécurité de votre navigateur peuvent empêcher l'exécution de scripts provenant des clients qui sont utilisés par Server Administrator. Pour activer l'utilisation de scripts provenant des clients, effectuez les étapes suivantes sur le système de gestion distant.

REMARQUE : Si vous n'avez pas configuré votre navigateur pour l'utilisation de scripts provenant des clients, un écran vide peut s'afficher lorsque vous ouvrez une session sur Server Administrator. Si c'est le cas, un message d'erreur vous invitant à configurer les paramètres de votre navigateur s'affiche.

Internet Explorer

1. Dans votre navigateur Web, cliquez sur **Outils**→ **Options Internet**→ **Sécurité**.
2. Cliquez sur l'icône **Sites de confiance**.
3. Cliquez sur **Sites**.
4. Copiez l'adresse Web utilisée pour accéder au système géré distant depuis la barre d'adresse du navigateur et collez-la dans le champ **Ajouter ce site Web à la zone**.
5. Cliquez sur **Personnaliser le niveau**.

   Pour Windows Server 2003 :

   - Sous **Divers**, sélectionnez le bouton radio **Permettre l'actualisation meta**.
   - Sous **Scripts actifs**, sélectionnez le bouton radio **Activer**.
   - Sous **Scripts actifs**, sélectionnez le bouton radio **Permettre les scripts des commandes de navigation Web d'Internet Explorer**.
6. Cliquez sur **OK** pour sauvegarder les nouveaux paramètres. Fermez le navigateur et ouvrez une session Server Administrator.

Pour permettre la connexion directe à Server Administrator sans demander les références de l'utilisateur, effectuez les étapes suivantes :

1. Dans votre navigateur Web, cliquez sur **Outils**→ **Options Internet**→ **Sécurité**.
2. Cliquez sur l'icône **Sites de confiance**.
3. Cliquez sur **Sites**.
4. Copiez l'adresse Web utilisée pour accéder au système géré distant depuis la barre d'adresse du navigateur et collez-la dans le champ **Ajouter ce site Web à la zone**.
5. Cliquez sur **Personnaliser le niveau**.
6. Sous **Authentification d'utilisateur**, sélectionnez le bouton radio **Connexion automatique avec le nom d'utilisateur et le mot de passe actuels**.
7. Cliquez sur **OK** pour sauvegarder les nouveaux paramètres.
8. Fermez le navigateur et ouvrez une session Server Administrator.

Mozilla Firefox

1. Démarrez votre navigateur.
2. Cliquez sur **Modifier**→ **Préférences**.
3. Cliquez sur **Avancés**→ **Scripts et plug-ins**.
4. Assurez-vous que la case à cocher **Navigateur** est sélectionnée sous **Activer JavaScript pour**.
5. Cliquez sur **OK** pour sauvegarder 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 la barre d'outils de votre navigateur Web (comme **Précédent** et **Actualiser**) lorsque vous utilisez Server Administrator. N'utilisez que les outils de navigation de Server Administrator.

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

- La zone barre de navigation globale<par défaut font> fournit des liens vers des services généraux.
- La zone arborescence du système<par défaut font> affiche tous les objets système visibles en fonction des privilèges d'accès de l'utilisateur.
- La zone fenêtre d'action<par défaut font> affiche les actions de gestion disponibles pour l'objet de l'arborescence du système sélectionné en fonction des privilèges d'accès de l'utilisateur. La fenêtre d'action contient trois zones opérationnelles :
  - Les onglets d'action affichent les actions principales ou les catégories d'action qui sont 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 zone de données<par défaut font> affiche des informations sur l'objet de l'arborescence du système sélectionné, l'onglet d'action et la sous-catégorie 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.

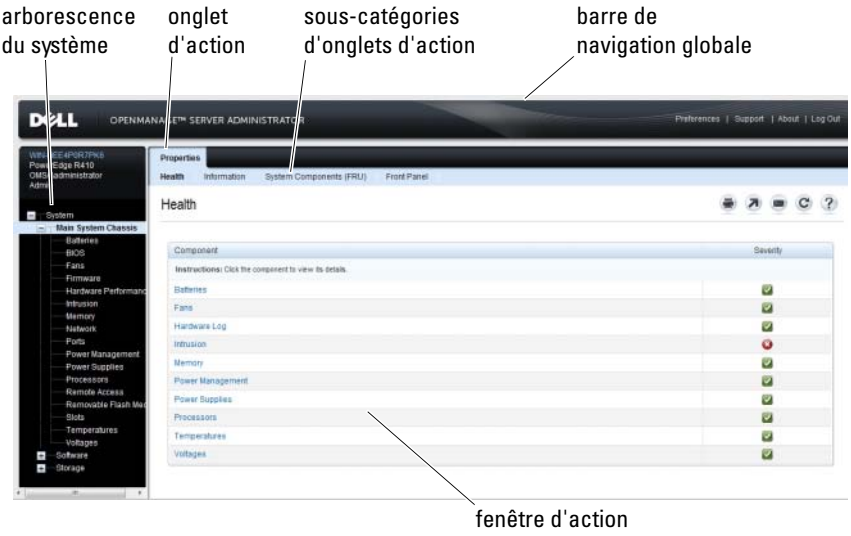
Le Tableau 3-1 répertorie les noms des champs de l'IUG et le système concerné, lorsque Server Administrator est installé sur le système.

Tableau 3-1. Disponibilité du système pour les noms des champs de l'interface utilisateur suivants

Nom de champ de l'interface utilisateur	Système concerné
`Enceinte modulaire`	Système modulaire
`Module de serveur`	Système modulaire
`Système principal`	Système modulaire
`Système`	Système non modulaire
`Châssis principal du système`	Système non modulaire

La Figure 3-1 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 3-1. Exemple de page d'accueil de Server Administrator — Système non modulaire



La Figure 3-2 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 3-2. Exemple de page d'accueil de Server Administrator — Système modulaire

Si vous cliquez sur un objet dans l'arborescence du système, la fenêtre d'action qui correspond à cet objet s'ouvre. Vous pouvez naviguer dans la fenêtre d'action en cliquant sur les onglets d'action pour sélectionner les catégories principales et sur les sous-catégories des onglets d'action pour accéder à des informations plus détaillées ou à des actions plus précises. Les informations affichées dans la zone de données de la fenêtre d'action peuvent comprendre les journaux du système, les indicateurs de condition et les niveaux des sondes du système. Les éléments soulignés dans la zone de données de la fenêtre d'action indiquent un niveau de fonctionnalité plus détaillé. Si vous cliquez sur un élément souligné, une nouvelle zone de données qui contient plus de détails apparaît dans la fenêtre d'action. Par exemple, si vous cliquez sur **Châssis principal du système/Système principal** dans la sous-catégorie **Intégrité** de l'onglet d'action **Propriétés**, une liste apparaît, donnant la condition d'intégrité de tous les composants contenus dans l'objet Châssis principal du système/Système principal dont la condition d'intégrité est surveillée.

REMARQUE : Les privilèges d'administrateur ou d'utilisateur privilégié sont requis pour pouvoir visualiser la plupart des objets de l'arborescence du système, les composants système, les onglets d'action et les fonctionnalités des zones de données qui sont configurables. De plus, seuls les utilisateurs connectés avec des privilèges d'administrateur peuvent accéder aux fonctionnalités critiques du système, comme la fonctionnalité d'arrêt comprise sous l'onglet **Arrêt**.

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

Tableau 3-2 répertorie la disponibilité des fonctionnalités de Server Administrator au sein des systèmes modulaires et non modulaires. Une marque de graduation indique la disponibilité, tandis qu'une croix indique la non disponibilité de la fonctionnalité.

Tableau 3-2. Différences d'interface utilisateur de Server Administrator au sein des systèmes modulaires et non modulaires

Fonctionnalités	Système modulaire	Système non modulaire
Batteries	✓	✓
Blocs d'alimentation	✗	✓
Ventilateurs	✗	✓
Performances du matériel	✗	✓ **(à partir de la version *xx0x* du système)**
Intrusion	✗	✓
Mémoire	✓	✓
Réseau	✓	✓
Ports	✓	✓
Power Management (Gestion de l'alimentation)	✓	✓ **(à partir de la version *xx0x* du système)**
Processeurs	✓	✓
Accès à distance	✓	✓
Média Flash amovible	✓	✓
Logements	✓	✓
Températures	✓	✓
Tensions	✓	✓
Enceinte modulaire (Informations sur le châssis et sur CMC)	✓	✗

Barre de navigation globale

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

- Cliquez sur **Préférences** pour ouvrir la page d'accueil **Préférences**. Voir « Utilisation de la page d'accueil Préférences<Par défaut Font> ».
- Cliquez sur **Support** pour établir une connexion au site Web de support Dell.
- 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 du système

L'arborescence du système, qui apparaît sur le côté gauche de la page d'accueil de Server Administrator, répertorie les composants de votre système qui peuvent être affichés. Les composants du système sont classés par type de composant. Lorsque vous développez l'objet principal connu comme **Enceinte modulaire→ Système/Module de serveur**, les principales catégories de composants du système/module de serveur susceptibles d'apparaître sont **Châssis principal du système/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 une entrée développée qui ne peut pas l'être davantage.

Fenêtre d'action

Lorsque vous cliquez sur un élément de l'arborescence du système, les détails sur le composant ou l'objet apparaissent dans la zone de données de la fenêtre d'action. Si vous cliquez sur un onglet d'action, toutes les options de l'utilisateur disponibles s'affichent dans une liste de sous-catégories.

Si vous cliquez sur un objet de l'arborescence du système/module de serveur, la fenêtre d'action de ce composant s'ouvre et affiche les onglets d'action disponibles. Par défaut, la zone de données passe à une sous-catégorie présélectionnée du premier onglet d'action correspondant à l'objet sélectionné. La sous-catégorie présélectionnée est généralement la première option. Par exemple, si vous cliquez sur l'objet **Châssis principal du système/Système principal**, une fenêtre d'action s'ouvre, dans laquelle l'onglet d'action **Propriétés** et la sous-catégorie **Intégrité** sont affichés dans la zone de données de la fenêtre.

Zone de données

La zone de données se situe sous les onglets d'action sur le côté droit de la page d'accueil. La zone de données vous permet d'effectuer des tâches ou d'afficher des détails sur des composants du système. Le contenu de la fenêtre dépend de l'objet de l'arborescence du système et de l'onglet d'action sélectionnés. Par exemple, si vous sélectionnez **BIOS** dans l'arborescence du système, l'onglet **Propriétés** est sélectionné par défaut et les informations sur la 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 fonctionnalités courantes, notamment les indicateurs de condition, 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 à côté des noms des composants indiquent la condition de ce composant particulier (telle qu'elle était au dernier rafraîchissement de la page).

Tableau 3-3. Indicateurs de condition des composants de système/module de serveur

	le composant est intègre (normal).
	le composant présente une condition d'avertissement (non critique). Une condition d'avertissement se produit lorsqu'une sonde ou un autre outil de surveillance détecte une mesure sur un composant qui atteint certaines valeurs minimales ou maximales. Une condition d'avertissement exige une intervention rapide.
	le component présente une condition d'échec ou critique. Une condition critique se produit lorsqu'une sonde ou un autre outil de surveillance détecte une mesure sur un composant qui atteint certaines valeurs minimales ou maximales. Une condition critique exige une intervention immédiate.
	la condition d'intégrité du composant est inconnu.

Boutons de tâches

La plupart des fenêtres ouvertes à partir de la page d'accueil de Server Administrator contiennent au moins cinq boutons de tâches : **Imprimer**, **Exporter**, **E-mail, Aide** et **Actualiser**. D'autres boutons de tâches sont inclus dans des fenêtres particulières de Server Administrator. Les fenêtres de journaux, par exemple, contiennent également les boutons de tâches **Enregistrer sous** et **Effacer le journal**.

- Si vous cliquez sur **Imprimer**, () une copie de la fenêtre ouverte est imprimée sur votre imprimante par défaut.
- Si vous cliquez sur **Exporter**, () un fichier texte répertoriant les valeurs de tous les champs de données de la fenêtre ouverte est généré. Le fichier exporté est enregistré dans l'emplacement que vous spécifiez. Voir « Configuration des préférences utilisateur et système » pour des instructions sur la personnalisation du délimiteur séparant les valeurs des champs de données.
- Si vous cliquez sur **E-mail**, (), un message e-mail adressé au destinataire d'e-mail de votre choix est créé. Voir « Configuration des préférences utilisateur et système » pour des instructions sur la configuration de votre serveur de messagerie et du destinataire d'e-mail par défaut.
- Si vous cliquez sur **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 **Enregistrer sous**, un fichier HTML de la fenêtre d'action est enregistré dans un fichier **.zip**.
- Si vous cliquez sur **Effacer le journal**, tous les événements du journal affichés dans la zone de données de la fenêtre d'action sont supprimés.
- Si vous cliquez sur **Aide** (), des informations détaillées concernant la fenêtre spécifique ou le bouton de tâche affiché apparaissent.

REMARQUE : Les boutons **Exporter, E-mail, Enregistrer sous** et **Effacer le journal** ne s'affichent que pour les utilisateurs connectés avec des privilèges d'administrateur ou d'utilisateur privilégié.

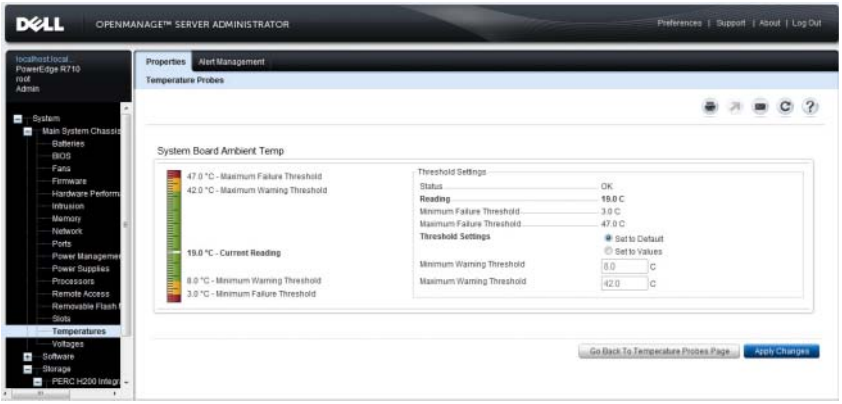
Éléments soulignés

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 sondes de température, les sondes de ventilateur et les sondes de tension sont représentées par un indicateur de niveau. Par exemple, la Figure 3-3 illustre les mesures d'une sonde de ventilateur de l'UC du système.

Figure 3-3. Indicateur de niveau



Utilisation de l'aide en ligne

Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. En cliquant sur **Aide** sur la barre de navigation globale, vous pouvez ouvrir une fenêtre d'aide indépendante contenant des informations détaillées sur la fenêtre spécifique que vous consultez. L'aide en ligne est conçue pour donner des conseils spécifiques sur les actions à prendre pour mener à bien toutes les phases 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 privilèges d'utilisateur.

Utilisation de la page d'accueil Préférences

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

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

- Paramètres généraux
- Server Administrator

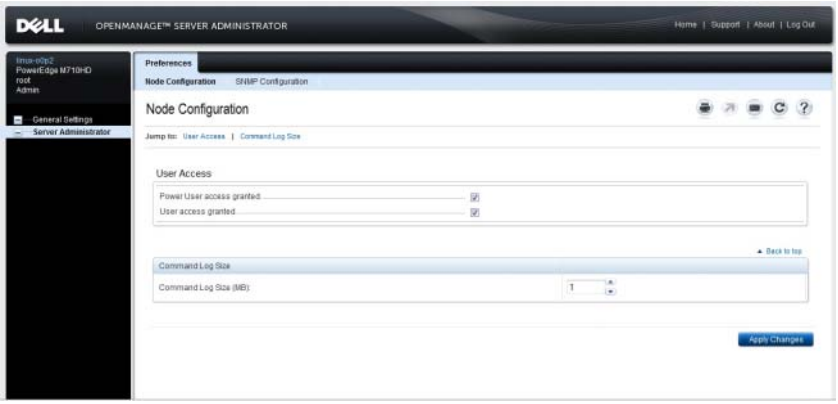
Vous pouvez afficher l'onglet **Préférences** une fois la session ouverte pour gérer un système distant. Cet onglet est également disponible lorsque vous ouvrez une session pour gérer Server Administrator Web Server ou le système local.

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

- La barre de navigation globale fournit des liens aux services généraux.
  - Cliquez sur **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.

Figure 3-4 affiche un exemple de page d'accueil Préférences.

Figure 3-4. Exemple de page d'accueil Préférences - Système géré



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 disposant de privilèges d'utilisateur ou d'utilisateur privilégié. Selon les privilèges de groupe de l'utilisateur, la fenêtre d'action de l'objet Server Administrator peut intégrer l'onglet **Préférences**.

Sous l'onglet Préférences, vous pouvez :

- Activer ou désactiver l'accès pour les utilisateurs ayant des privilèges d'utilisateur ou d'utilisateur privilégié.
- 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 **Préférences** revient par défaut à la fenêtre **Préférences utilisateur** sous l'onglet Préférences.

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 Gérer Web Server :

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

Pour plus d'informations sur l'accès à ces fonctionnalités, consultez « Services Server Administrator ».

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

Configuration des préférences utilisateur et système

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

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

Procédez comme suit pour configurer vos préférences utilisateur :

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

   La page d'accueil **Préférences** apparaît.

2. Cliquez sur **Paramètres généraux**.
3. Pour ajouter un destinataire d'e-mail présélectionné, tapez l'adresse e-mail de votre contact désigné pour le service dans le champ **Destinataire**, puis cliquez sur **Appliquer les changements**.

   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.

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

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

   La page d'accueil **Préférences** apparaît.

2. Cliquez sur **Paramètres généraux**, puis sur l'onglet **Web Server**.

3 Dans la fenêtre **Préférences serveur**, définissez les options souhaitées.

- La fonctionnalité **Délai d'expiration de la session** permet de limiter la durée d'activation d'une session Server Administrator. Sélectionnez le bouton radio **Activer** pour que la session Server Administrator expire si elle n'est pas utilisée pendant un nombre de minutes déterminé. Les utilisateurs dont la session expire doivent se reconnecter pour pouvoir continuer. Sélectionnez le bouton radio **Désactiver** pour désactiver la fonctionnalité d'expiration de session de Server Administrator.
- Le champ **Port HTTPS** spécifie le port sécurisé de Server Administrator. Le port sécurisé par défaut de Server Administrator est 1311.

REMARQUE : Si vous donnez un numéro de port qui n'est pas valide ou qui est déjà utilisé, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré. Consultez le *Guide d'installation et de sécurité de Dell OpenManage* pour obtenir la liste des ports par défaut.

- Le champ **Associer à l'adresse IP** précise la ou les adresses IP du système géré auxquelles Server Administrator s'associe lors de l'ouverture d'une session. Sélectionnez le bouton radio **Toutes** pour pouvoir associer toutes les adresses IP qui s'appliquent à votre système. Sélectionnez le bouton radio **Spécifique** pour associer à une adresse IP spécifique.

REMARQUE : Si vous donnez à la valeur **Associer à l'adresse IP** une autre valeur que **Toutes**, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré.

- Le champ **Envoyer l'e-mail à** indique les ID d'email auxquels les emails sur les mises à jour seront envoyés par défaut. Vous pouvez configurer plusieurs ID d'e-mail en les séparant par une virgule.
- Les champs **Nom du serveur SMTP** et **Suffixe DNS du serveur SMTP** spécifient le protocole de transfert de courrier simple (SMTP) et le suffixe du serveur de noms de domaine (DNS) de votre entreprise ou organisation. Pour que Server Administrator puisse envoyer des e-mails, vous devez taper l'adresse 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 **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 **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 avec le bouton **Exporter**. Le caractère **;** est le délimiteur par défaut. Les autres options sont !, @, #, $, %, ^, *, ~, ?, | et ,.
- Le champ **Cryptage SSL** spécifie les niveaux de cryptage des sessions HTTPS sécurisées. Les niveaux de cryptage disponibles sont **Négociation automatique** et **128 bits ou plus**.
  - **Négociation automatique** : permet une connexion à partir d'un navigateur avec n'importe quel niveau de cryptage. Le navigateur négocie automatiquement avec le serveur Web de Server Administrator et utilise le niveau de cryptage disponible le plus élevé pour la session. Les navigateurs hérités ayant des niveaux de cryptage plus faibles peuvent se connecter à Server Administrator.
  - **128 bits ou plus** : permet des connexions à partir de navigateurs ayant un niveau de cryptage de 128 bits ou plus élevé. Une des suites de chiffrement suivantes s'applique à la session établie, en fonction de votre navigateur :

    SSL_RSA_WITH_RC4_128_SHA
    SSL_RSA_WITH_RC4_128_MD5
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
    TLS_RSA_WITH_AES_128_CBC_SHA
    TLS_DHE_DSS_WITH_AES_128_CBC_SHA
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

- **Algorithme de signature de clé** : affiche les algorithmes de signature pris en charge. Sélectionnez un algorithme dans la liste déroulante. Si vous sélectionnez SHA 512 ou SHA 256, assurez-vous que votre système d'exploitation/navigateur prend en charge cet algorithme. Si vous sélectionnez l'une de ces options sans la prise en charge du système d'exploitation/navigateur requis, Server Administrator affiche l'erreur : « `Impossible d'afficher la page Web` ». Ce champ est destiné uniquement aux certificats auto-signés de Server Administrator générés automatiquement. La liste déroulante est grisée si vous importez ou générez de nouveaux certificats dans Server Administrator.

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

REMARQUE : Vous devez redémarrer le serveur Web de Server Administrator pour appliquer les changements.

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

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

Gestion du certificat X.509

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

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

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

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

Les options disponibles sont les suivantes :

- **Générer un nouveau certificat X.509** : crée un certificat d'accès à Server Administrator.
- **Maintenance de certificat** : cette option sélectionne un certificat existant qui appartient à votre société et qu'elle utilise pour contrôler l'accès à Server Administrator.
- **Importer un certificat racine** : cette option vous permet d'importer le certificat racine, ainsi que la réponse du certificat (au format PKCS#7) reçue de la part de l'autorité de certification approuvée.
- **Importer une chaîne de certificats d'une autorité de certification** : cette option vous permet d'importer la réponse du certificat (au format PKCS#7) de l'autorité de certification approuvée. Parmi les autorités de certification fiables, citons Verisign, Thawte et Entrust.

Onglets d'action de Server Administrator Web Server

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

- Arrêt
- Journaux
- Gestion des sessions

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

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

Dans de nombreux cas, la CLI permet à l'utilisateur ayant une tâche bien spécifique à l'esprit de récupérer rapidement les informations du système. Les commandes CLI, par exemple, permettent aux administrateurs d'écrire des programmes ou des scripts de commandes pour pouvoir les exécuter à un moment précis. Lorsque ces programmes s'exécutent, ils peuvent capturer des rapports sur les composants présentant un intérêt, comme par exemple le nombre de tours par minute des ventilateurs. Avec des scripts supplémentaires, la CLI peut être utilisée pour capturer des données pendant des périodes de forte utilisation du système pour les comparer aux mesures équivalentes relevées à des périodes de faible utilisation du système. Les résultats des commandes peuvent être acheminés vers un fichier pour être analysés plus tard. Les rapports peuvent permettre aux administrateurs d'obtenir des informations qui peuvent être utilisées pour ajuster les habitudes d'utilisation, justifier l'achat de nouvelles ressources système ou focaliser l'attention sur l'intégrité d'un composant problématique.

Pour des instructions complètes sur la fonctionnalité et l'utilisation de la CLI, consultez le *Guide d'utilisation de l'interface de ligne de commande de Dell OpenManage Server Administrator.*

4

Services Server Administrator

Présentation

Le service Dell OpenManage Server Administrator Instrumentation Service surveille l'intégrité d'un système et fournit un accès rapide aux informations détaillées sur les défaillances et les performances recueillies par les agents de gestion de systèmes standard de l'industrie. Les fonctions de compte rendu et d'affichage vous permettent d'obtenir la condition d'intégrité générale de chacun des châssis qui composent votre système. Au niveau du sous-système, vous pouvez afficher les informations sur les tensions, les températures, le nombre de tours/minute des ventilateurs et la mémoire à des points clés du système. L'affichage du résumé vous permet d'obtenir un rapport détaillé sur tous les faits concernant le coût de possession (CDP) de votre système. Vous pouvez facilement obtenir des informations sur les versions du BIOS, des micrologiciels, du système d'exploitation et du logiciel Systems Management installé.

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

- Définir les valeurs minimales et maximales de certains composants critiques. Les valeurs, appelées seuils, déterminent la plage à l'intérieur de laquelle un événement d'avertissement se produit pour ce composant (les valeurs minimales et maximales de panne sont définies par le fabricant du système).
- Définir la réponse du système lorsqu'un événement d'avertissement ou de panne se produit. Les utilisateurs peuvent configurer les mesures prises par un système en réponse aux notifications d'avertissement et de panne. Les utilisateurs qui bénéficient d'une surveillance permanente peuvent aussi faire en sorte qu'aucune action ne soit prise et se fier au jugement humain pour choisir la meilleure action possible en réponse à un événement.
- Remplir toutes les valeurs définissables par l'utilisateur pour le système, par exemple, le nom du système, le numéro de téléphone de l'utilisateur principal du système, la méthode d'amortissement, si le système est loué ou acheté, et ainsi de suite.

REMARQUE : Vous devez configurer le service SNMP (Simple Network Management Protocol [Protocole simplifié de gestion de réseau]) pour accepter les paquets SNMP à la fois pour les systèmes gérés et pour les stations de gestion de réseau fonctionnant sous Microsoft Windows Server 2003. Voir Configuration de l'agent SNMP pour les systèmes fonctionnant sous un système d'exploitation Windows pris en charge pour plus d'information.

Gestion de votre système

La page d'accueil de Server Administrator s'ouvre par défaut sur l'objet **Système** de l'arborescence du système. Par défaut, l'objet **Système** s'ouvre sur les composants **Intégrité** sous l'onglet **Propriétés**.

La page d'accueil des **préférences** est par défaut la fenêtre **Configuration de l'accès** sous l'onglet **Préférences**.

Dans la page d'accueil **Préférences**, 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 DSM SA.

REMARQUE : Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. Cliquez sur **Aide** pour ouvrir une fenêtre d'aide indépendante qui contient des informations détaillées sur cette fenêtre. L'aide en ligne est conçue pour donner des conseils spécifiques sur les actions à prendre pour mener à bien toutes les phases 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 privilèges d'utilisateur.

REMARQUE : Des privilèges d'administrateur ou d'utilisateur privilégié sont requis pour pouvoir accéder à de nombreux objets de l'arborescence du système, aux composants système, aux onglets d'action et aux fonctionnalités des zones de données qui sont configurables. De plus, seuls les utilisateurs connectés avec des privilèges d'administrateur peuvent accéder aux fonctionnalités critiques du système, comme la fonctionnalité d'arrêt comprise sous l'onglet **Arrêt**.

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

L'arborescence de système/module de serveur de Server Administrator affiche tous les objets visibles du système en fonction des groupes logiciels et matériels que Server Administrator découvre sur le système géré et en fonction des privilèges d'accès de l'utilisateur. Les composants du système sont classés par type de composant. Lorsque vous développez l'objet principal— « **Enceinte modulaire** » — « **Système/Module de serveur** » — les principales catégories de composants du système qui peuvent apparaître sont « **Châssis principal du système/Système principal** », « **Logiciel** » et « **Stockage** ».

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

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

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

Fonctionnalités non prises en charge dans OpenManage Server Administrator

En raison des limitations des systèmes d'exploitation VMware ESX et ESXi, version 4.X et 5.X, certaines fonctionnalités disponibles dans les versions antérieures d'OpenManage Server Administrator ne sont pas disponibles dans la présente version. Celles-ci incluent :

Fonctionnalités non prises en charge sur ESX 4.X

- Informations sur les capacités Fibre Channel sur Ethernet (FCoE) et iSCSI sur Ethernet (iSoE)

Fonctionnalités non prises en charge sur ESXi 4.X/5.X

- Informations sur les capacités FCoE et iSoE
- Gestion des alertes : Actions d'alerte
- Interface réseau : Condition d'administration
- Interface réseau : DMA
- Interface réseau : Adresse du protocole Internet (IP)
- Interface réseau : Unité de transmission maximale
- Interface réseau : Condition d'exploitation
- Préférences : Configuration SNMP
- Arrêt distant : Système de cycle d'alimentation avec arrêt du SE en premier
- Á propos des détails : Les détails du composant Server Administrator ne sont pas répertoriés sous l'onglet **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 pouvoir accéder à de nombreux objets de l'arborescence du système, aux composants système, aux onglets d'action et aux fonctionnalités des zones de données configurables. De plus, seuls les utilisateurs connectés avec des privilèges d'administrateur peuvent accéder aux fonctionnalités critiques du système, comme la fonctionnalité d'arrêt comprise sous l'onglet **Arrêt**.

Enceinte modulaire

REMARQUE : Dans Server Administrator, l'expression *« enceinte modulaire »* fait référence à un système pouvant contenir un ou plusieurs systèmes modulaires apparaissant en tant que module de serveur séparé dans l'arborescence du système. Tout comme un module de serveur autonome, une enceinte modulaire contient tous les composants essentiels d'un système. Seule différence, une enceinte modulaire comporte des logements pour au moins deux modules de serveurs dans un plus grand conteneur et chacun d'eux est un système aussi complet qu'un 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** Enceinte modulaire.

Propriétés

Sous-onglets : Informations

Sous l'onglet **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** Chassis Management Controller depuis la page d'accueil de Server Administrator :

1. Cliquez sur l'objet **Enceinte modulaire.**
2. Cliquez sur l'onglet **Information CMC**, puis cliquez sur **Lancer l'interface Web CMC**. La fenêtre d'**ouverture de session** CMC est affichée.

Vous pouvez surveiller et gérer votre enceinte modulaire après vous être connecté à CMC.

Système/Module de serveur

L'objet **Système/Module de serveur** contient trois principaux groupes de composants du système : « Châssis principal du système/Système principal », « Logiciel » et « Stockage ». La page d'accueil de Server Administrator revient par défaut à l'objet **Système** de l'affichage de l'arborescence du système. La plupart des fonctions administratives peuvent être gérées à partir de 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, selon les privilèges de groupe de l'utilisateur : **Propriétés**, **Arrêt**, **Journaux**, **Gestion des alertes** et **Gestion des sessions**.

Propriétés

Sous-onglets : Intégrité | Résumé | Informations sur l'inventaire | Récupération automatique

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

- Afficher la condition actuelle des alertes d'intégrité pour les composants matériels et logiciels de l'objet **Châssis principal du système/Système principal** et de l'objet **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 Récupération automatique du système peuvent ne pas être disponibles si le registre d'horloge de la surveillance du système d'exploitation est activé dans le BIOS. Pour configurer les options de récupération automatique, vous devez désactiver le registre d'horloge de la surveillance du système d'exploitation.

  REMARQUE : Les actions de récupération automatique du système peuvent ne pas s'exécuter suivant le délai d'attente imparti (n secondes) quand la surveillance identifie un système qui ne répond plus. Le temps d'exécution des actions s'étend de *n-h+1* à *n+1* secondes, où *n* est le temps d'attente et *h* est l'intervalle de pulsation. La valeur de l'intervalle de pulsation est 7 secondes quand $n \leq 30$ et 15 secondes quand $n > 30$.

  REMARQUE : La fonctionnalité du registre d'horloge de la surveillance ne peut pas être garantie si un événement de mémoire ne pouvant pas être corrigé se produit dans le banc de mémoire 1 de la DRAM du système. S'il y a effectivement un tel événement, le code BIOS du banc risque de se corrompre. Parce que la fonctionnalité de surveillance utilise un appel au BIOS pour effectuer un arrêt ou un redémarrage, cette fonctionnalité peut ne pas fonctionner correctement. Si cela se produit, vous devez redémarrer manuellement le système. Vous pouvez définir le registre d'horloge de la surveillance sur un maximum de 720 secondes.

Arrêt

Sous-onglets : 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 se produit si la température rapportée par le capteur dépasse le seuil de température. Il n'y a pas d'arrêt thermique si la température rapportée par le capteur descend en dessous du seuil de température.

- Arrêter le service de connexion DSM SA (serveur Web).

  REMARQUE : Server Administrator demeure disponible via l'interface de ligne de commande (CLI) lorsque le service de connexion DSM SA est arrêté. Le service de connexion DSM SA n'a pas besoin d'être démarré pour utiliser les fonctions de la CLI .

Journaux

Sous-onglets : Matériel | Alerte | Commande

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

- Afficher le journal de gestion de système intégrée (ESM) ou le journal d'événements du système (SEL) pour afficher une liste de tous les événements associés aux composants matériels de votre système. L'icône d'indicateur d'état en regard du nom du journal passe d'une condition normale () à une condition non critique () lorsque le fichier journal atteint une capacité de 80 %. Sur les systèmes Dell PowerEdge*x9xx* et *xx1x*, l'icône d'indicateur d'état en regard du nom du journal se transforme en condition critique () lorsque le fichier journal atteint une capacité de 100 %.

  REMARQUE : Nous vous conseillons d'effacer le journal du matériel lorsqu'il est rempli à 80 %. Si le journal atteint une capacité de 100 %, les événements les plus récents ne sont pas journalisés.

- 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 : Consultez le *Guide de référence des messages de Server Administrator* pour obtenir une explication détaillée de la description, du niveau de gravité et de la cause correspondant à chaque ID d'événement d'alerte.

- 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 : Consultez « Journaux de Server Administrator » pour obtenir des instructions détaillées sur l'affichage, l'impression, l'enregistrement et l'envoi par e-mail des journaux.

Gestion des alertes

Sous-onglets : Actions d'alerte | Événements sur plateforme| Interruptions SNMP

Sous l'onglet **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 tous les paramètres actuels des filtres d'événements de plateforme et définir les actions de filtrage d'événements de plateforme à effectuer si le capteur d'un composant du système donne 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 une alerte concernant un événement sur plateforme sera envoyée.

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

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

  REMARQUE : Les actions d'alerte de tous les capteurs potentiels des composants du système sont répertoriées dans la fenêtre **Actions d'alerte**, même si elles ne sont pas présentes sur votre système. La définition des actions d'alertes pour des capteurs de composants du système qui ne sont pas sur votre système n'a aucun effet.

Gestion des sessions

Sous-onglets : Session

Sous l'onglet **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 des sessions et mettre fin aux sessions des utilisateurs connectés.

Châssis principal du système/Système principal

Cliquez sur l'objet **Châssis principal du système/Système principal** pour gérer les composants matériels et logiciels principaux de votre système.

Les composants disponibles sont :

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

REMARQUE : Performances du matériel : ce composant est pris en charge uniquement sur les systèmes Dell PowerEdge *xx0x* et versions ultérieures. les blocs d'alimentation ne sont pas disponibles sur le système Dell PowerEdge 1900. Gestion de l'alimentation : ce composant est pris en charge sur certains systèmes Dell PowerEdge *xx0x* et versions ultérieures. Les fonctionnalités Surveillance du bloc d'alimentation et Surveillance de l'alimentation sont uniquement disponibles pour les systèmes sur lesquels au moins deux blocs d'alimentation remplaçables à chaud redondants sont installés. Ces fonctionnalités ne sont pas disponibles pour des blocs d'alimentation non redondants installés de manière permanente et ne disposant pas de circuit de gestion de l'alimentation.

Le système/module de serveur peut contenir un châssis principal du système ou plusieurs châssis. Le châssis principal du système/système principal contient les composants principaux d'un système. La fenêtre d'action de l'objet **Châssis principal du système/Système principal** comporte l'onglet suivant : **Propriétés**.

Propriétés

Sous-onglets : Intégrité | Informations | Composants du système (FRU) | Panneau avant

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

- Afficher l'intégrité ou la condition des composants matériels et des capteurs. Chaque composant répertorié a une icône « Indicateurs de condition des composants de système/module de serveur » en regard de son nom.  indique qu'un composant est intègre (normal).  indique qu'une condition d'avertissement (non critique) est associée à un composant et que ce composant nécessite une intervention.  indique qu'une condition de panne (critique) est associée à un composant et que ce composant nécessite une intervention immédiate.  indique que la condition d'un composant est inconnue. Parmi les composants surveillés disponibles :
  - Batteries
  - Ventilateurs
  - Journal du matériel
  - Intrusion
  - Mémoire
  - Réseau
  - Power Management (Gestion de l'alimentation)
  - Blocs d'alimentation
  - Processeurs
  - Températures
  - Tensions

REMARQUE : Les batteries sont prises en charge uniquement sur les systèmes Dell PowerEdge *x9xx* et Dell *xx0x*.
Le composant « Blocs d'alimentation » n'est pas disponible sur le système Dell PowerEdge 1900.
Le composant « Gestion de l'alimentation » n'est pris en charge que sur certains systèmes Dell *xx0x* limités. Les fonctionnalités Surveillance du bloc d'alimentation et Surveillance de l'alimentation sont uniquement disponibles pour les systèmes sur lesquels au moins deux blocs d'alimentation remplaçables à chaud redondants sont installés. Ces fonctionnalités ne sont pas disponibles pour des blocs d'alimentation non redondants installés de manière permanente et ne disposant pas de circuit de gestion de l'alimentation.

REMARQUE : Si l'adaptateur de bus hôte (HBA) Fibre Channel à port unique 4 Gb QLE2460 QLogic, le HBA Fibre Channel double port 4 Gb QLE2462 QLogic, le FC8 double port QLE2562 Qlogic, ou les cartes adaptateur FC8 à port unique QLE2560 Qlogic sont installées sur les systèmes yx2x, l'écran Composants système (FRU) ne s'affiche pas.

- Afficher des informations concernant les attributs du châssis du système principal, par exemple le Nom d'hôte, la version iDRAC, la version Lifecycle Controller, le modèle du châssis, le verrouillage du châssis, le numéro de service du châssis, le code de service express et le numéro d'inventaire du châssis. L'attribut de Code de service express (ESC) est une conversion numérique uniquement de 11 chiffres du numéro de service du système Dell. Pour que votre appel soit automatiquement acheminé lorsque vous appelez le Support technique Dell, saisissez cet attribut à l'aide des touches du téléphone.
- Affichez des informations détaillées concernant les unités remplaçables sur site (FRU) installées sur votre système (sous le sous-onglet **Composants système (FRU)**.)
- Activez ou désactivez les boutons du panneau avant du système géré, à savoir le bouton d'alimentation et le bouton d'interruption non masquable (NMI) (s'il y en a un sur le système). Sélectionnez également le niveau Accès de sécurité de l'écran LCD du système géré. Vous pouvez sélectionner les informations relatives à l'écran LCD du système géré dans le menu déroulant. Vous pouvez également activer Indication de session KVM distant dans le sous-onglet **Panneau avant**.

Batteries

Cliquez sur l'objet **Batteries** pour afficher les informations sur les batteries installées de votre système. Les batteries conservent la date et l'heure auxquelles votre système est éteint. La batterie enregistre la configuration du BIOS du système, ce qui permet au système de redémarrer efficacement. La fenêtre d'action de l'objet **Batteries** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglet : Informations

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

Gestion des alertes

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

BIOS

Cliquez sur l'objet **BIOS** pour gérer les fonctionnalités clés du BIOS de votre système. Le BIOS de votre système contient des programmes, enregistrés sur un chipset de mémoire flash, qui contrôlent la communication entre le microprocesseur et les périphériques, par exemple, le clavier et la carte vidéo, et d'autres fonctions diverses, telles que les messages du système. La fenêtre d'action de l'objet **BIOS** peut présenter les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Configuration**.

Propriétés

Sous-onglet : Informations

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

Configuration

Sous-onglet : BIOS

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

Vous pouvez modifier la condition de nombreuses fonctionnalités de configuration du BIOS, dont notamment le port série, la séquence de lecteur de disque dur, les ports USB accessibles aux utilisateurs, la technologie de virtualisation de l'UC, l'hyperthreading de l'UC, le mode de restauration de l'alimentation en CA, le contrôleur SATA intégré, le profil du système, la redirection de console et le débit en bauds fiable de la redirection de console. Vous pouvez également configurer un périphérique USB interne, les paramètres du contrôleur de disque optique, le registre d'horloge de la surveillance de récupération automatique du système (ASR), l'hyperviseur intégré et des informations supplémentaires sur les ports du réseau local (LAN) de la carte-mère. Vous pouvez afficher les paramètres du module de plateforme sécurisé (TPM) et du module cryptographique sécurisé (TCM).

Selon la configuration spécifique de votre système, des éléments de configuration supplémentaires peuvent être affichés. Néanmoins, certaines options de configuration du BIOS affichées sur l'écran de configuration du BIOS F2 peuvent ne pas être accessibles dans Server Administrator.

Pour les systèmes yx2x, les fonctionnalités configurables du BIOS sont regroupées et forment des catégories spécifiques. Ces catégories incluent : Informations sur le système, Paramètres de mémoire, Paramètres du profil du système, Paramètres d'amorçage UEFI (Unified Extensible Firmware Interface), Cartes réseau (NIC), Amorçage Ponctuel et Désactivation de logement. Par exemple, sur la page **Paramètres du BIOS?du système**, lorsque vous cliquez sur le lien **Paramètres de mémoire**, les fonctionnalités correspond à la mémoire du système s'affichent. Vous pouvez voir ou modifier les paramètres en naviguant vers les catégories respectives.

Vous pouvez définir un mot de passe de configuration du BIOS sur la page **Configuration du BIOS - Sécurité du système**. Vous devez saisir le mot de passe pour activer et modifier les paramètres BIOS. Sinon, les paramètres du BIOS?apparaissent en mode lecture seule. Vous devez redémarrer 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 portant sur la configuration des NIC dans l'écran de configuration du **BIOS** de Server Administrator peuvent être inexactes pour les NIC intégrés. L'utilisation de l'écran de configuration du **BIOS** pour activer ou désactiver les NIC peut produire des résultats inattendus. Nous vous conseillons d'effectuer toutes les configurations des NIC intégrées dans l'écran **Configuration du système** ; vous pouvez y accéder en appuyant sur <F2> au démarrage du système.

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

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/minute de chaque ventilateur. Les sondes des ventilateurs fournissent le nombre de tours/minute des ventilateurs à Server Administrator Instrumentation Service. 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 : Capteurs de ventilateurs

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

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

  REMARQUE : Certains champs de sonde de ventilateur diffèrent en fonction du type de micrologiciel dont votre système dispose : BMC ou ESM. Certaines valeurs de seuils ne peuvent pas être modifiées sur les systèmes basés sur le contrôleur BMC.

- Sélectionner les options de contrôle des ventilateurs.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **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.
- Afficher les seuils actuels des alertes d'interruption SNMP et définir les niveaux des seuils d'alerte des ventilateurs. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Micrologiciel

Cliquez sur l'objet **Micrologiciel** pour gérer le micrologiciel de votre système. Un micrologiciel est composé de programmes ou de données écrits dans la mémoire morte. Le micrologiciel peut démarrer et faire fonctionner un périphérique. Chaque contrôleur contient un micrologiciel qui aide à donner au contrôleur sa fonctionnalité. La fenêtre d'action de l'objet **Micrologiciel** peut avoir l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

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

Performances du matériel

Cliquez sur l'objet **Performances du matériel** pour afficher la condition et la cause de la dégradation des performances du système. La fenêtre d'action de l'objet **Performances du matériel** peut avoir l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Tableau 4-1 répertorie les valeurs possibles pour la condition et la cause d'une sonde :

Tableau 4-1. Valeurs possibles pour la condition et la cause d'une sonde

Valeurs de condition	Valeurs de cause
Dégradé	Configuration de l'utilisateur
	Capacité d'alimentation insuffisante
	Raison inconnue
Normal	[N/A]

Propriétés

Sous-onglet : Informations

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

Intrusion

Cliquez sur l'objet **Intrusion** pour gérer la condition d'intrusion dans le châssis de votre système. Server Administrator surveille la condition d'intrusion dans le châssis par mesure de sécurité pour empêcher l'accès non autorisé aux composants critiques de votre système. L'intrusion dans le châssis indique si le capot du châssis du système est ou a été ouvert. La fenêtre d'action de l'objet **Intrusion** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglet : Intrusion

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

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **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 d'intrusion donne une valeur d'avertissement ou de panne.
- Afficher les seuils actuels des alertes d'interruption SNMP et définir les niveaux des seuils d'alerte du 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 **Mémoire** pour gérer les périphériques de mémoire de votre système. Server Administrator surveille la condition des périphériques de mémoire pour chaque module de mémoire installé sur le système surveillé. Les capteurs de panne anticipée des périphériques de mémoire surveillent les modules de mémoire en comptant le nombre de corrections de mémoire ECC. Server Administrator surveille aussi les informations sur la redondance de mémoire si cette fonctionnalité est prise en charge par votre système. La fenêtre d'action de l'objet **Mémoire** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés et Gestion des alertes**.

Propriétés

Sous-onglet : Mémoire

Sous l'onglet **Propriétés**, vous pouvez afficher les conditions 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 les conditions des périphériques de mémoire.

REMARQUE : Si un système avec un banc mémoire de réserve activé entre dans un état de perte de la redondance, il est difficile d'identifier le module de mémoire qui en est la cause. Si vous ne pouvez pas déterminer la DIMM à remplacer, consultez l'entrée de journal *passage vers banc mémoire de réserve détecté* dans le journal ESM du système pour trouver quel module de mémoire est défaillant.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **Gestion des alertes**, vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si un module de mémoire donne une valeur d'avertissement ou de panne.
- Afficher les seuils actuels des alertes d'interruption 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 installé sur votre système pour assurer une connexion à distance ininterrompue. Dell OpenManage Server Administrator rapporte les capacités FCoE et iSoE des NIC. Les détails de regroupements de NIC sont rapportés s'ils sont déjà configurés sur le système. Deux NIC physiques, ou plus, peuvent être regroupées pour former une NIC logique unique, à laquelle un administrateur est à même d'attribuer une adresse IP. Le regroupement peut être configuré à l'aide des outils de fournisseurs de NIC. Par exemple, Broadcom - BACS. Si l'une des NIC physiques échoue, l'adresse IP reste accessible car elle est liée à la NIC logique, et non à une seule NIC physique. Si l'interface du groupe est configurée, les propriétés détaillées du groupe s'affichent. La relation entre les NIC physiques et l'interface du groupe, et inversement, est également signalée, à condition que ces NIC physiques soient membres de l'interface du groupe.

REMARQUE : L'ordre dans lequel les périphériques sont détectés ne correspond pas nécessairement à l'ordre des ports physiques du périphérique. Cliquez sur le lien hypertexte sous le nom de l'interface pour afficher les informations NIC.

Dans le cas de systèmes d'exploitation ESX and ESXi, le périphérique réseau est considéré comme un groupe. Par exemple, l'interface Ethernet virtuel utilisée par la Service Console (vswif) et l'interface de réseau virtuel utilisée par les périphériques VMKernel (vmknic) sur ESX, et le périphérique vmknic sur ESXi.

La fenêtre d'action de l'objet **Réseau** peut présenter l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **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 « Adresses IPv6 », Server Administrator affiche uniquement deux adresses, en plus de l'adresse locale du lien.

Ports

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

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 fonctionnalités Surveillance du bloc d'alimentation et Surveillance de l'alimentation sont uniquement disponibles pour les systèmes sur lesquels au moins deux blocs d'alimentation remplaçables à chaud redondants sont installés. Ces fonctionnalités ne sont pas disponibles pour des blocs d'alimentation non redondants installés de manière permanente et ne disposant pas de circuit de gestion de l'alimentation.

Surveillance

Sous-onglets : Consommation | Statistiques

Dans l'onglet 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 afficher la hauteur instantanée du système et la hauteur maximale du système. Les valeurs sont affichées en watts et BTU/h (British Thermal Unit). Les seuils d'alimentation peuvent être définis en watts et BTU/h.

L'onglet 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 : Bilan | Profils

L'onglet Bilan vous permet d'afficher les attributs d'inventaire d'alimentation comme la puissance système en veille et la puissance potentielle maximale du système, en watts et BTU/h. Vous pouvez également utiliser l'option Bilan de puissance pour activer le plafond de puissance et définir le plafond de puissance de votre système.

L'onglet 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 : Actions d'alerte | Interruptions SNMP

Utilisez l'onglet 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 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 les blocs d'alimentation installés sur votre système fonctionnent 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 fonctionnalités Surveillance du bloc d'alimentation et Surveillance de l'alimentation sont uniquement disponibles pour les systèmes sur lesquels au moins deux blocs d'alimentation remplaçables à chaud redondants sont installés. Ces fonctionnalités ne sont pas disponibles pour des blocs d'alimentation non redondants installés de manière permanente et ne disposant pas de circuit de gestion de l'alimentation.

Propriétés

Sous-onglet : Éléments

Sous l'onglet **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 du micrologiciel du bloc d'alimentation, la puissance d'entrée nominale et la puissance de sortie maximale. L'attribut de puissance d'entrée nominale s'affiche uniquement sur les systèmes PMBus à partir de la version *xx1x*.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **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 actuels d'alerte des interruptions SNMP et définir les niveaux des seuils d'alerte des watts d'alimentation du système. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

REMARQUE : L'interruption de puissance système maximale génère des événements uniquement pour la gravité de niveau Informatif.

Processeurs

Cliquez sur l'objet **Processeurs** pour gérer les microprocesseurs de votre système. Un processeur est la puce de traitement principale d'un système ; il contrôle l'interprétation et l'exécution des fonctions mathématiques et logiques. La fenêtre d'action de l'objet **Processeurs** peut présenter les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglet : Informations

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 : 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 **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 Accès à distance permet de gérer les fonctionnalités BMC/iDRAC telles que les informations générales sur le contrôleur BMC/iDRAC. Vous pouvez aussi gérer la configuration du contrôleur BMC/iDRAC sur un réseau local (LAN), le port série pour le contrôleur BMC/iDRAC, les paramètres du mode terminal du port série, les connexions série sur le réseau local du contrôleur BMC/iDRAC et les utilisateurs du contrôleur BMC/iDRAC.

REMARQUE : Le contrôleur BMC est pris en charge par les systèmes Dell PowerEdge *x9xx*, et le contrôleur iDRAC est pris en charge par les systèmes Dell *xx0x* et *xx1x* uniquement.

REMARQUE : Si une application différente de Server Administrator sert à configurer le contrôleur BMC/iDRAC pendant que Server Administrator est en cours d'exécution, les données de configuration du contrôleur BMC/iDRAC affichées par Server Administrator peuvent devenir asynchrones par rapport au contrôleur BMC/iDRAC. Il est recommandé d'utiliser Server Administrator pour configurer le contrôleur BMC/iDRAC pendant que Server Administrator est en cours d'exécution.

Le contrôleur DRAC vous permet d'accéder aux capacités de gestion de système distante de votre système. Server Administrator DRAC fournit un accès distant aux systèmes non opérationnels, une notification d'alerte lorsqu'un système est hors service et la possibilité de redémarrer un système.

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

Propriétés

Sous-onglet : Informations

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

Cliquez sur **Restaurer les valeurs par défaut** pour réinitialiser tous les attributs sur leurs valeurs système par défaut.

Configuration

Sous-onglets : Réseau local | Port série | Connexion série sur le réseau local | Configuration supplémentaire

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

REMARQUE : L'onglet **Configuration supplémentaire** est disponible uniquement sur les systèmes dotés du contrôleur iDRAC.

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

REMARQUE : Les champs **Activer la NIC**, **Sélection de NIC** et **Clé de cryptage** ne s'affichent que sur les systèmes Dell PowerEdge *x9xx*.

Sous l'onglet 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 : Utilisateurs

Sous l'onglet **Utilisateurs**, vous pouvez modifier la configuration des utilisateurs de l'accès distant. Vous pouvez ajouter, configurer et consulter les informations sur les utilisateurs de Remote Access Controller.

REMARQUE : Sur les systèmes Dell PowerEdge *x9xx* :
- Dix ID d'utilisateur s'affichent. Si une carte DRAC est installée, seize ID d'utilisateur s'affichent.
- La colonne Charge utile des communications série sur le LAN s'affiche.

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 du média flash amovible comporte un onglet **Propriétés**.

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, vous pouvez afficher des informations à propos du média flash amovible et des modules SD internes. Ceci inclut des détails sur le nom du connecteur, son état et sa taille de stockage.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **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 retourne une valeur d'avertissement ou de panne.

- Afficher les seuils d'alerte actuels des interruptions SNMP et définir les niveaux des seuils d'alerte des capteurs du média flash amovible. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

La gestion des alertes est commune aux modules SD internes et au média vFlash. La configuration d'actions d'alerte/SNMP/PEF pour les modules SD, ou pour le média vFlash, est automatiquement répercutée sur l'autre ou les autres, selon le cas.

Logements

Cliquez sur l'objet **Logements** pour gérer les connecteurs ou supports pour cartes à circuits imprimés (comme les cartes d'extension) de votre carte système. La fenêtre d'action de l'objet **Logements** comporte l'onglet **Propriétés**.

Propriétés

Sous-onglet : Informations

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

Températures

Cliquez sur l'objet **Températures** pour gérer la température de votre système afin d'éviter l'endommagement thermique de ses composants internes. 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**.

Propriétés

Sous-onglet : Sondes de température

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

REMARQUE : Certains champs de sonde de température diffèrent en fonction du type de micrologiciel dont votre système dispose : BMC ou ESM. Certaines valeurs de seuils ne peuvent pas être modifiées sur les systèmes basés sur le contrôleur BMC. Lors de l'attribution des valeurs des seuils des sondes, Server Administrator arrondit parfois les valeurs minimales et maximales que vous saisissez.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **Gestion des alertes**, vous pouvez :

- Afficher tous les paramètres actuels des actions d'alerte et définir les actions d'alerte à effectuer si une sonde de température renvoie une valeur d'avertissement ou de panne.
- Afficher les seuils d'alerte actuels des interruptions SNMP et définir les niveaux des seuils d'alerte des sondes 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 minimales et maximales des seuils des capteurs de température pour un châssis externe sur des nombres entiers uniquement. Si vous tentez de définir la valeur minimale ou maximale des seuils des capteurs de température sur un nombre décimal, seul le nombre entier avant la virgule est enregistré comme paramètre de seuil.

Tensions

Cliquez sur l'objet **Tensions** pour gérer les niveaux des tensions à l'intérieur de votre système. Server Administrator surveille les tensions des composants critiques à plusieurs endroits du châssis dans le système surveillé. La fenêtre d'action de l'objet **Tensions** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglet : Sondes de tension

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

REMARQUE : Certains champs de sonde de tension diffèrent en fonction du type de micrologiciel dont votre système dispose : BMC ou ESM. Certaines valeurs de seuils ne peuvent pas être modifiées sur les systèmes basés sur le contrôleur BMC.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

Sous l'onglet **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 tension du système renvoie une valeur d'avertissement ou de panne.
- Afficher les seuils actuels d'alerte des interruptions SNMP et définir les niveaux des seuils d'alerte des capteurs de tension. Les interruptions sélectionnées sont déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

Logiciel

Cliquez sur l'objet **Logiciels** pour afficher des informations détaillées sur la version des composants logiciels principaux du système géré, tels que le système d'exploitation et le logiciel de gestion du système. La fenêtre d'action de l'objet **Logiciels** comporte l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Résumé

Sous l'onglet **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 sur votre système d'exploitation. La fenêtre d'action de l'objet **Système d'exploitation** comporte l'onglet suivant, selon les 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) :

Storage Management Service offre des fonctionnalités pour la configuration des périphériques de stockage. Dans la plupart des cas, Storage Management Service s'installe à l'aide de l'option **Installation par défaut**. 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 **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 **Stockage** comporte l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : 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 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 affichées sont fonction du logiciel Systems Management installé sur le système géré.

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

- Paramètres généraux
- Server Administrator

Paramètres généraux

Cliquez sur l'objet **Paramètres généraux** pour définir les préférences utilisateur et du service de connexion DSM SA (serveur Web) pour les fonctions de Server Administrator sélectionnées. La fenêtre d'action de l'objet **Paramètres généraux** présente les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Utilisateur** et **Serveur Web**.

Utilisateur

Sous-onglet : Propriétés

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

Serveur Web

Sous-onglets : Propriétés | Certificat X.509

Sous l'onglet **Serveur Web**, vous pouvez :

- Définir les préférences du service de connexion DSM SA. Consultez « Service de connexion Dell Systems Management Server Administration et configuration de la sécurité » pour obtenir des instructions pour la configuration de vos préférences de serveur.
- Configurer l'adresse de serveur SMTP et l'adresse IP de liaison dans le mode d'adressage IPv4 ou IPv6.
- Gérer le certificat X.509 en générant un nouveau certificat X.509, en réutilisant un certificat X.509 existant ou en important un certificat racine ou une chaîne de certificat d'une autorité de certification (CA). Pour plus d'informations sur la gestion des certificats, voir « Gestion du certificat X.509 », à la page 67.

Server Administrator

Cliquez sur l'objet **Server Administrator** pour activer ou désactiver l'accès pour les utilisateurs ayant des privilèges d'utilisateur ou d'utilisateur privilégié, et pour configurer le mot de passe root (racine) SNMP. La fenêtre d'action de l'objet **Server Administrator** peut présenter l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Préférences**.

Préférences

Sous-onglets : Configuration de l'accès | Configuration SNMP

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

- Activer ou désactiver l'accès pour les utilisateurs ayant des privilèges d'utilisateur ou d'utilisateur privilégié.
- Configurer le mot de passe root SNMP.

REMARQUE : L'utilisateur par défaut pour la configuration SNMP est `root` et le mot de passe est `calvin`.

- Configurer les opérations Set SNMP (Configurer SNMP).

REMARQUE : Après avoir configuré les opérations Set SNMP, vous devez redémarrer les services pour que les changements deviennent effectifs. Sur les systèmes fonctionnant sous un système d'exploitation Microsoft Windows pris en charge, le service SNMP Windows doit être redémarré. Sur les systèmes fonctionnant sous des systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge, les services Server Administrator doivent être redémarrés en exécutant la commande `srvadmin-services.sh restart`.

5

Utilisation de Remote Access Controller

REMARQUE : *Le contrôleur de gestion de la carte mère (BMC)* est pris en charge par les systèmes Dell PowerEdge *x*9xx, et le contrôleur *Integrated Dell Remote Access Controller (iDRAC)* est pris en charge par les systèmes Dell *xx0x* et *xx1x*.

Présentation

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

Les contrôleurs Baseboard Management Controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) des systèmes Dell surveillent le système afin de détecter les événements critiques en communiquant avec divers capteurs de la carte système. Ces contrôleurs envoient des alertes et des événements journalisés lorsque certains paramètres dépassent leurs seuils prédéfinis. Les contrôleurs BMC/iDRAC prennent en charge la spécification Interface de gestion de plate-forme intelligente (IPMI) standard de l'industrie, vous permettant de configurer, de surveiller et de récupérer des systèmes à distance.

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

En communiquant avec les contrôleurs de gestion de la carte mère (BMC)/Integrated Dell Remote Access Controller (iDRAC) du système, le DRAC peut être configuré pour vous envoyer des alertes par e-mail concernant les avertissements ou les erreurs liés aux tensions, températures et vitesses de ventilateur. Le DRAC consigne également les données d'événements et l'écran de panne le plus récent (pour les systèmes fonctionnant sous le système d'exploitation Microsoft Windows uniquement) pour vous aider à diagnostiquer la cause probable d'une panne du système.

Remote Access Controller permet d'accéder à distance à un système inutilisable et vous permet ainsi de réparer et de reconnecter ce système aussi vite que possible. Remote Access Controller permet aussi de signaler quand un système est éteint et de le redémarrer à distance. Remote Access Controller consigne également la cause probable des pannes du système et enregistre l'*écran de panne le plus récent*.

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

Lorsque vous utilisez Remote Access Controller, vous pouvez cliquer sur **Aide** sur la barre de navigation globale pour obtenir des informations plus détaillées sur la fenêtre visualisée. L'aide de Remote Access Controller est disponible pour toutes les fenêtres accessibles à l'utilisateur selon le niveau de privilèges de l'utilisateur et les groupes particuliers de matériel et de logiciels que Server Administrator découvre sur le système géré.

REMARQUE : Consultez le *Guide d'utilisation des utilitaires de contrôleur de gestion de la carte mère* de *Dell OpenManage* pour des informations supplémentaires sur le contrôleur BMC.

REMARQUE : Voir le *Guide d'utilisation de Dell Remote Access Controller 5* pour plus d'informations sur l'utilisation de DRAC 5.

REMARQUE : Consultez le Guide d'utilisation d'*Integrated Dell Remote Access Controller* pour obtenir des informations détaillées sur la configuration et l'utilisation du contrôleur iDRAC.

Le Tableau 5-1 répertorie les noms des champs de l'IUG et le système concerné, lorsque Server Administrator est installé sur le système.

Tableau 5-1. Disponibilité du système pour les noms des champs de l'IUG suivants

Nom de champ de l'interface utilisateur	Système concerné
`Enceinte modulaire`	Système modulaire
`Modules serveurs`	Système modulaire
`Système principal`	Système modulaire
`Système`	Système non modulaire
`Châssis principal du système`	Système non modulaire

Voir la *matrice de prise en charge des logiciels système Dell* disponible sur le site **support.dell.com** pour plus d'informations sur la prise en charge des systèmes concernant les périphériques d'accès à distance.

Server Administrator permet un accès à distance intrabande aux journaux d'événements, au contrôle de l'alimentation et aux informations sur la condition des capteurs tout en permettant de configurer les contrôleurs BMC/iDRAC. Vous pouvez gérer les contrôleurs BMC/iDRAC et DRAC via l'interface utilisateur graphique de Server Administrator en cliquant sur l'objet **Accès à distance** qui est un sous-composant du groupe **Châssis principal du système/Système principal**.

Vous pouvez réaliser les tâches suivantes :

- Afficher les informations de base
- Configurer le périphérique d'accès à distance sur une connexion LAN
- Configurer le périphérique d'accès à distance sur une connexion par communication série sur le LAN
- Configurer le périphérique d'accès à distance sur une connexion par port série
- Configurer des propriétés de périphérique d'accès à distance supplémentaires
- Configurer des utilisateurs sur le périphérique d'accès à distance
- Définir des alertes de filtre d'événements sur plate-forme

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

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

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

REMARQUE : Vous pouvez consulter les données du contrôleur BMC sur les systèmes Dell PowerEdge *x9xx* uniquement.

Affichage des informations de base

Vous pouvez afficher les informations de base sur le contrôleur BMC/iDRAC, l'adresse IPv4 et DRAC. Vous pouvez également rétablir les valeurs par défaut des paramètres de Remote Access Controller. Pour ce faire :

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

Cliquez sur l'objet **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.

La page **Accès à distance** affiche les informations essentielles suivantes sur le contrôleur BMC de votre système :

Périphérique d'accès à distance

- Type de périphérique
- Version d'IPMI
- GUID système
- Nombre de sessions actives possibles
- Nombre de sessions actives en cours
- Activé sur le LAN
- SOL activé
- Adresse MAC

Adresse IPv4

- IP Address Source (Source d'adresse IP)
- Adresse IP
- Sous-réseau IP
- Passerelle IP

Adresse IPv6

- IP Address Source (Source d'adresse IP)
- Adresse IPv6 1
- Passerelle par défaut
- Adresse IPv6 2
- Adresse locale de liaison

- Source d'adresse DNS
- Serveur DNS préféré
- Autre serveur DNS

REMARQUE : Vous pouvez afficher les détails relatifs aux adresses IPv4 et IPv6 uniquement si vous activez les propriétés d'adresses IPv4 et IPv6 sous **Configuration supplémentaire** dans l'onglet **Accès à distance**.

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 **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Réseau local (LAN)**.

   La fenêtre **Configuration du réseau local (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 (cette option est disponible sur les systèmes Dell PowerEdge *x9xx*, lorsque le contrôleur DRAC est installé). Sélectionnez cette option pour le regroupement des NIC. Sur les systèmes Dell PowerEdge *x9xx*, vous pouvez regrouper les NIC pour une redondance accrue.)

     REMARQUE : Votre contrôleur DRAC contient un NIC Ethernet intégré 10BASE-T/100BASE-T et prend en charge TCP/IP. Par défaut, le NIC doit avoir l'adresse par défaut 192.168.20.1 et la passerelle par défaut 192.168.20.1.

     REMARQUE : Si votre contrôleur DRAC est configuré sur la même adresse IP qu'un autre NIC du même réseau, un conflit d'adresse IP se produit. Le contrôleur DRAC cesse de répondre aux commandes du réseau tant que l'adresse IP du contrôleur DRAC n'est pas modifiée. Le contrôleur DRAC doit être réinitialisé même si le conflit d'adresse IP est résolu en changeant l'adresse IP de l'autre NIC.

REMARQUE : La modification de l'adresse IP du contrôleur DRAC provoque la réinitialisation du contrôleur DRAC. Si SNMP interroge le contrôleur DRAC avant de s'initialiser, un avertissement de température est consigné car la température correcte n'est transmise qu'après l'initialisation du contrôleur DRAC.

– NIC Selection (Sélection de NIC)

REMARQUE : **Sélection de NIC** ne peut pas être configurée sur les systèmes modulaires.

REMARQUE : L'option **Sélection de NIC** est disponible sur les systèmes yx1x et de version antérieure uniquement.

– Options de réseau principal et de basculement

Pour les systèmes yx2x, les options de **Primary Network** (Réseau principal) pour la NIC de Remote Management (iDRAC7) sont les suivantes : LOM1, LOM2, LOM3, LOM4 et Dédié. Les options de **réseau de basculement** sont: LOM1, LOM2, LOM3, LOM4, All LOMs et Aucun.

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

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

– Activer IPMI sur LAN
– IP Address Source (Source d'adresse IP)
– Adresse IP
– Masque de sous-réseau
– Adresse de passerelle
– Limite du niveau de privilège du canal
– Nouvelle clé de cryptage (cette option est disponible sur les systèmes Dell PowerEdge *x9xx*).

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 est installé le contrôleur iDRAC

– Activer le numéro VLAN
– Identifiant du VLAN
– Priority (Priorité)

6 Configurez les propriétés IPv4 suivantes :
   – IP Address Source (Source d'adresse IP)
   – Adresse IP
   – Masque de sous-réseau
   – Adresse de passerelle
7 Configurez les propriétés IPv6 suivantes :
   – IP Address Source (Source d'adresse IP)
   – Adresse IP
   – Longueur du préfixe
   – Passerelle par défaut
   – Source d'adresse DNS
   – Serveur DNS préféré
   – Autre serveur DNS

   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 **Configuration supplémentaire**.
8 Cliquez sur **Apply Changes** (Appliquer les modifications).

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 l'objet **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.
2 Cliquez sur l'onglet **Configuration**.
3 Cliquez sur **Port série**.
   La fenêtre **Configuration du port série** apparaît.
4 Configurez les détails suivants :
   – Paramètre du mode de connexion
   – Baud Rate (Débit en bauds)

- Contrôle du débit
- Limite du niveau de privilège du canal

5 Cliquez sur **Appliquer les modifications**.

6 Cliquez sur **Paramètres du mode terminal**.

Dans la fenêtre **Paramètres du mode terminal**, vous pouvez configurer les paramètres du mode terminal pour le port série.

Le mode terminal est utilisé pour la messagerie IPMI (gestion de l'interface de plate-forme intelligente) sur le port série à l'aide de caractères ASCII imprimables. Le mode terminal prend aussi en charge un nombre limité de commandes texte pour prendre en charge les environnements classiques basés sur texte. Cet environnement est conçu de sorte à permettre l'utilisation d'un terminal simple ou d'un émulateur de terminal.

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 l'établissement de liaisons
- Nouvelle séquence linéaire
- Saisie d'une nouvelle séquence linéaire

8 Cliquez sur **Appliquer les modifications**.

9 Cliquez sur **Retourner à la fenêtre Configuration du port série** pour revenir à la fenêtre **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 **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.

2 Cliquez sur l'onglet **Configuration**.

3 Cliquez sur **Communications série sur le LAN**.

La fenêtre **Configuration de la connexion série sur le réseau local (LAN)** apparaît.

4 Configurez les détails suivants :

- Activation des communications série sur LAN
- Débit en bauds
- Privilèges minimum requis

5 Cliquez sur **Appliquer les modifications**.

6 Cliquez sur **Paramètres avancés** pour configurer le contrôleur BMC.

7 Dans la fenêtre **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 modifications**.

9 Cliquez sur **Retourner à la configuration de la connexion série sur le réseau local** pour revenir à la fenêtre **Configuration de la connexion série sur le réseau local**.

Configuration supplémentaire pour iDRAC

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

1 Cliquez sur l'objet **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.

2 Cliquez sur l'onglet **Configuration**.

3 Cliquez sur **Configuration supplémentaire**.

4 Configurez les propriétés IPv4 et IPv6 en les définissant sur **Activé** ou **Désactivé**.

5 Cliquez sur **Appliquer les modifications**.

Pour plus d'informations sur la gestion de licences, voir le *Guide d'utilisation de Dell License Manager* disponible sur le site **support.dell.com**.

Configuration des utilisateurs du périphérique d'accès à distance

Pour configurer les utilisateurs du périphérique Remote Access à l'aide de la page **Remote Access** :

1. Cliquez sur l'objet **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.
2. Cliquez sur l'onglet **Utilisateurs**.

   La fenêtre **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 **ID d'utilisateur** pour configurer un nouvel utilisateur des contrôleurs BMC/iDRAC ou un utilisateur existant.

   La fenêtre **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 **Activer l'utilisateur** pour activer l'utilisateur.
   - Entrez le nom de l'utilisateur dans le champ **Nom d'utilisateur**.
   - Cochez la case **Modifier le mot de passe**.
   - Entrez un nouveau mot de passe dans le champ **Nouveau mot de passe**.
   - Entrez de nouveau le nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe**.
5. Spécifiez les privilèges d'utilisateur suivants :
   - Sélectionnez la limite maximale de privilèges utilisateur sur le réseau local.
   - Sélectionnez la limite maximale de privilèges utilisateur sur le port série accordée.
   - Sur les systèmes Dell PowerEdge *x9xx* , sélectionnez **Activer les communications série sur le LAN** pour activer les communications série sur le LAN.

6 Spécifiez le groupe d'utilisateurs pour les privilèges d'utilisateur des contrôleurs DRAC/iDRAC.

7 Cliquez sur **Appliquer les modifications** pour enregistrer les modifications.

8 Cliquez sur **Retour à la fenêtre Utilisateurs de l'accès à distance** pour retourner à la fenêtre **Utilisateurs de l'accès à distance**.

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

Définition des alertes de filtre d'événements sur plateforme

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

1 Cliquez sur l'objet **Système**.

2 Cliquez sur l'onglet **Gestion des alertes**.

3 Cliquez sur **Événements sur plateforme**.

La fenêtre **Événements sur plateforme** permet d'effectuer des actions individuelles sur des événements de plate-forme spécifiques. Vous pouvez sélectionner les événements sur lesquels vous voulez effectuer des actions d'arrêt et générer des alertes pour les actions sélectionnées. Vous pouvez aussi envoyer des alertes à des destinations d'adresse IP spécifiques de votre choix.

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

REMARQUE : Le paramètre **Activer les alertes des filtres d'événements sur plateforme** active ou désactive la génération d'alertes de filtre d'événements sur plateforme. Il est indépendant des paramètres d'alerte d'événement de plate-forme individuels.

REMARQUE : Avertissement de capteur de puissance système et Panne de capteur de puissance système ne sont pas pris en charge par les systèmes Dell ne prenant pas en charge PMBus, bien que Server Administrator vous permette cette configuration.

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

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

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

5 Sélectionnez l'une des actions suivantes :

- **Aucun**
  Ne réagit pas si le système d'exploitation est bloqué ou s'il tombe en panne.
- **Redémarrer le système**
  Arrête le système d'exploitation et initialise un démarrage du système, en effectuant les vérifications du BIOS et en rechargeant le système d'exploitation.
- **Exécuter un cycle d'alimentation sur le système**
  Met le système hors tension, attend brièvement, le remet sous tension et le redémarre. Le cycle d'alimentation est utile si vous voulez réinitialiser des composants système comme, par exemple, les disques durs.
- **Arrêter le système**
  Met le système hors tension.
- **Réduction de puissance**
  Accélère l'UC.

PRÉCAUTION : Si vous sélectionnez une action d'arrêt d'événement de plateforme autre que Aucune ou Réduction de puissance , un arrêt forcé de votre système s'effectuera lorsque l'événement spécifié se produira. Cet arrêt est mis en œuvre par le micrologiciel et est effectué sans arrêter d'abord le système d'exploitation ou toute application en cours d'exécution.

REMARQUE : La réduction de l'alimentation n'est pas prise en charge sur tous les systèmes. Les fonctionnalités Surveillance des blocs d'alimentation et Surveillance de l'alimentation sont disponibles uniquement pour les systèmes sur lesquels au moins deux blocs d'alimentation redondants et échangeables à chaud sont installés. Ces fonctionnalités ne sont pas disponibles pour des blocs d'alimentation permanents, non redondants et ne disposant pas de circuit de gestion d'alimentation.

6 Cochez la case **Générer une alerte** pour les alertes à envoyer.

REMARQUE : Pour générer une alerte, vous devez à la fois sélectionner les paramètres **Générer une alerte** et **Activer les alertes d'événements de plateforme**.

7 Cliquez sur **Appliquer les modifications**.

8 Cliquez sur **Retour à la page Événements sur plateforme** pour revenir à la fenêtre **Filtres d'événements sur plateforme**.

Définition des destinations des alertes d'événements de plateforme

Vous pouvez également utiliser la fenêtre **Filtres d'événements sur plateforme** pour sélectionner une destination vers laquelle une alerte concernant une plateforme sera envoyée. En fonction du nombre de destinations qui s'affichent, vous pouvez configurer une adresse IP différente pour chaque adresse de destination. Une alerte d'événement sur plateforme est envoyée à chaque adresse IP de destination que vous configurez.

1 Cliquez sur **Configurer les destinations** dans la fenêtre **Filtres d'événements sur plateforme**.

La fenêtre **Configurer les destinations** affiche un nombre de destinations.

2 Cliquez sur le numéro de la destination que vous voulez configurer.

REMARQUE : Le nombre de destinations que vous pouvez configurer sur un système donné peut varier.

3 Cochez la case **Activer la destination**.

4 Cliquez sur **Numéro de destination** pour entrer une adresse IP individuelle pour cette destination. Cette adresse IP est l'adresse IP à laquelle l'alerte d'événement sur plateforme est envoyée.

5 Entrez une valeur dans le champ **Chaîne de communauté** qui joue le rôle de mot de passe pour authentifier les messages envoyés entre une station de gestion et un système géré. La chaîne de communauté (également appelée nom de communauté) est envoyée dans chaque paquet entre la station de gestion et le système géré.

6 Cliquez sur **Appliquer les modifications**.

7 Cliquez sur **Retour à la page Événements sur plateforme** pour revenir à la fenêtre **Filtres d'événements sur plateforme**.

6

Journaux de Server Administrator

Présentation

Server Administrator vous permet de visualiser et de gérer les journaux de matériel, des alertes et de commandes. Tous les utilisateurs peuvent accéder aux journaux et imprimer des comptes rendus depuis la page d'accueil de Server Administrator ou depuis son interface de ligne de commande. Les utilisateurs doivent ouvrir une session avec des droits d'administrateur pour effacer les journaux ou ouvrir une session avec des droits d'administrateur ou d'utilisateur privilégié pour envoyer les journaux par e-mail au contact du service désigné.

Consultez le *Guide d'utilisation de l'interface de ligne de commande de Dell OpenManage Server Administrator* à l'adresse **support.dell.com** pour obtenir des informations sur l'affichage des journaux et la création de comptes rendus depuis la ligne de commande.

Lors de l'affichage des journaux de Server Administrator, vous pouvez cliquer sur **Aide** dans la barre de navigation globale pour de plus amples informations sur la fenêtre que vous êtes en train de consulter. L'aide des journaux de Server Administrator est disponible pour toutes les fenêtres auxquelles l'utilisateur peut accéder en fonction de son niveau de privilège et des groupes de matériel et de logiciels spécifiques que Server Administrator découvre sur le système géré.

Fonctionnalités intégrées

Cliquez sur un titre de colonne pour trier selon cette colonne ou modifier le sens du tri de la colonne. De plus, chaque fenêtre de journal contient plusieurs boutons de tâche qui permettent la gestion et la prise en charge du système.

Boutons de tâche des fenêtres des journaux

- Cliquez sur **Imprimer** pour imprimer une copie du journal sur votre imprimante par défaut.
- Cliquez sur **Exporter** pour enregistrer un fichier texte contenant les données du journal (avec les valeurs des différents champs de données séparées par un délimiteur personnalisable) à un emplacement que vous spécifiez.

- Cliquez sur **E-mail** pour créer un message électronique comprenant le contenu du journal en pièce jointe.
- Cliquez sur **Effacer le journal** pour effacer tous les événements répertoriés dans le journal.
- Cliquez sur **Enregistrer sous** pour enregistrer le contenu du journal dans un fichier **.zip**.
- Cliquez sur **Actualiser** pour charger de nouveau le contenu du journal dans la zone de données de la fenêtre d'action.

Consultez « Boutons de tâches » pour obtenir des informations supplémentaires sur l'utilisation des boutons de tâche.

Journaux de Server Administrator

Server Administrator fournit les journaux suivants :

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

Journal du matériel

Utilisez le journal du matériel pour détecter les éventuels problèmes des composants matériels de votre système. Sur les systèmes Dell PowerEdge *x9xx* et *xx1x*, l'indicateur d'état du journal du matériel se transforme en condition critique () lorsque le fichier journal atteint une capacité de 100 %. Deux journaux du matériel sont disponibles selon votre système : le journal de gestion système intégrée (ESM) et le journal des événements système (SEL). Les journaux ESM et SEL contiennent chacun un jeu d'instructions intégrées qui peuvent envoyer des messages sur la condition du matériel au logiciel de gestion de systèmes. Chaque composant répertorié dans les journaux comporte une icône d'indicateur de condition à côté de son nom.
Une coche verte () indique que le composant est en bon état (normal). Un triangle jaune avec un point d'exclamation () indique que le composant est dans un état d'avertissement (non critique) et requiert une intervention rapide. Un X rouge () indique que le composant est dans un état de panne (critique) et requiert une intervention immédiate. Un espace vide () indique que la condition d'intégrité du composant n'est pas connue.

Pour accéder au journal du matériel, cliquez sur **Système**, puis sur l'onglet **Journaux** et sur **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 de l'indicateur d'état à côté du nom du journal dans 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 %. Effacez le journal du matériel lorsqu'il a atteint une capacité de 80 %. Si le journal atteint une capacité de 100 %, les événements les plus récents ne sont pas journalisés.

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 **Effacer le journal**, puis affichez à nouveau les informations du journal.

Utilisez le journal des alertes pour contrôler les divers événements du système. Server Administrator génère des événements en réponse aux changements de condition des capteurs et des autres paramètres surveillés. Chaque événement de changement de condition enregistré dans le journal des alertes est composé d'un identifiant unique appelé ID d'événement pour une catégorie source d'événement spécifique et d'un message d'événement décrivant l'événement. L'ID et le message d'événement décrivent de manière unique la gravité et la cause de l'événement, et fournissent d'autres informations pertinentes, par exemple l'emplacement de l'événement et l'état précédent du composant surveillé.

Pour accéder au journal des alertes, cliquez sur **Système**, puis sur l'onglet **Journaux** et sur **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 utile à des fins de dépannage ultérieur et de diagnostic. Par conséquent, il est recommandé d'enregistrer les fichiers journaux.

Pour en savoir plus sur les messages d'alerte, voir le *Guide de référence des messages Server Administrator* sur le site **support.dell.com**.

Journal de commandes

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

Utilisez le journal de commandes pour surveiller toutes les commandes émises par les utilisateurs de Server Administrator. Le journal de commandes identifie les ouvertures et fermetures de session, l'initialisation du logiciel de gestion des systèmes et les arrêts provoqués par le logiciel de gestion des systèmes, et enregistre le dernier effacement du journal. La taille du fichier journal de commandes peut être spécifiée en fonction de vos besoins.

Pour accéder au journal de commandes, cliquez sur **Système**, puis sur l'onglet **Journaux** et sur **Commande**.

Les informations affichées dans le journal de 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 utile à des fins de dépannage ultérieur et de diagnostic. Par conséquent, il est recommandé d'enregistrer les fichiers journaux.

7

Définition d'actions d'alerte

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

Lorsque vous définissez les actions d'alerte d'un événement, vous pouvez spécifier que l'action affiche une alerte sur le serveur. Pour effectuer cette action, Server Administrator envoie un message à **/dev/console**. Par défaut, ce message ne s'affiche pas si le système Server Administrator fonctionne sous un système X Window. Pour voir le message d'alerte sur un système Red Hat Enterprise Linux lorsque le système X Window s'exécute, vous devez lancer la commande **xconsole** ou **xterm -C** avant que l'événement ne se produise. Pour voir le message d'alerte sur un système SUSE Linux Enterprise Server zlorsque le système X Window s'exécute, vous devez lancer la commande **xterm -C** avant que l'événement ne se produise.

Lorsque vous définissez les actions d'alerte d'un événement, vous pouvez spécifier que l'action **diffuse un message**. Pour effectuer cette action, Server Administrator exécute la commande **wall** qui envoie le message à toutes les personnes connectées dont l'autorisation de messagerie est définie sur **Oui**. Par défaut, ce message ne s'affiche pas si le système Server Administrator fonctionne sous un système X Window. Pour afficher le message de diffusion quand le système X Windows s'exécute, 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 d'un événement, vous pouvez spécifier que l'action **exécute une application**. Il y a des limites aux applications que Server Administrator peut exécuter. Suivez les consignes suivantes pour que l'exécution soit correcte :

- Ne spécifiez pas d'applications de système X Window car Server Administrator est incapable d'exécuter ces applications correctement.
- Ne spécifiez pas d'applications qui nécessitent des entrées de la part de l'utilisateur car Server Administrator est incapable d'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 **Chemin absolu de l'application**.

  Exemple 1 :

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

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

  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 messagerie pour envoyer le message du fichier **/tmp/alertmsg.txt** à l'utilisateur et à l'administrateur de Red Hat Enterprise Linux ou SUSE Linux Enterprise Server, avec le sujet **Server Alert**. Le fichier **/tmp/alertmsg.txt** doit être créé par l'utilisateur avant que l'événement ne se produise. En cas d'erreur, **stdout** et **stderr** sont alors redirigés vers le fichier **/tmp/mailout.txt**.

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

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

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

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

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

Ne définissez pas un chemin vers une application interactive (une application qui comporte une interface utilisateur graphique ou qui nécessite une entrée de l'utilisateur) dans le champ Chemin absolu vers l'application. L'application interactive peut ne pas s'exécuter comme prévu sur certains systèmes d'exploitation.

REMARQUE : Vous devez spécifier le chemin complet vers le fichier cmd.exe et vers votre fichier de script.

REMARQUE : Microsoft Windows 2003 n'est pas pris en charge sur les systèmes yx2x.

Définition de l'application des actions d'alerte sous Windows Server 2008

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

Lorsque vous utilisez Server Administrator pour configurer les actions d'alerte pour un événement, vous pouvez spécifier que l'action *exécute une application*. Pour que des applications interactives puissent s'exécuter correctement pour une action d'alerte, le service Gestionnaire de données Dell Systems Management Server Administrator (DSM SA) doit être configuré comme service interactif. Des exemples d'applications interactives sont les applications ayant une interface utilisateur graphique (IUG) ou qui invitent l'utilisateur à entrer des données d'une certaine façon, par exemple via la commande *pause* dans un fichier séquentiel.

Lorsque Server Administrator est installé sur Microsoft Windows Server 2008, le service Gestionnaire de données DSM SA est installé comme service non interactif, ce qui signifie qu'il est configuré de manière à ne pas autoriser l'interaction avec le bureau par défaut. Cela signifie que les applications interactives ne s'exécutent pas correctement dans le cas des actions d'alerte. Si une application interactive est exécutée pour une action d'alerte dans cette situation, l'application est suspendue et attend une saisie. L'interface/l'invite de l'application n'est pas visible et reste invisible même après le démarrage du service de détection des services interactifs. L'onglet **Processus** dans **Gestionnaire des tâches** affiche une entrée de processus d'application pour chaque exécution de l'application interactive.

Si vous avez besoin d'exécuter une application interactive pour une action d'alerte sur Microsoft Windows Server 2008, vous devez configurer le service Gestionnaire de données DSM SA pour être autorisé l'interaction avec le bureau.

Pour autoriser l'interaction avec le bureau :

1. Cliquez avec le bouton droit de la souris sur le service Gestionnaire de données DSM SA dans le volet **Contrôle des services**, puis sélectionnez **Propriétés**.
2. Dans l'onglet **Ouvrir une session**, sélectionnez **Autoriser le service à interagir avec le Bureau** et cliquez sur **OK**.
3. Redémarrez le service Gestionnaire de données DSM SA pour que le changement puisse être effectif.
4. Assurez-vous que le service **Interactive Services Detection** est en cours d'exécution.

Lorsque vous redémarrer le service DSM SA Data Manager avec ce changement, la gestion de contrôle de service journalise le message suivant sur le journal du système :

```
Le service DSM SA Data Manager est marqué en tant que
service interactif.  Activer le service Interactive
Services Detection (détection des services
interactifs) permet au service DSM SA Data Manager
d'exécuter correctement des applications interactives
pour une action d'alerte.
```

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

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

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

Tableau 7-1. Événements d'alerte PEF

Évènement	Description
Panne de sonde de ventilateur	Le ventilateur fonctionne trop lentement ou pas du tout.
Panne de sonde de tension	La tension est trop basse pour un fonctionnement correct.
Avertissement de capteur de batterie	La batterie fonctionne en dessous du niveau de charge recommandé.
Panne de capteur de batterie	Échec de la batterie.
Échec discret signalé par le capteur de tension	La tension est trop basse pour un fonctionnement correct.
Avertissement de capteur de température	La température approche de ses limites excessivement hautes ou basses.
Panne de capteur de température	La température est trop haute ou trop basse pour un fonctionnement correct.
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 a été réduite.
Redondance (bloc d'alimentation ou ventilateur) dégradée	Plus aucune redondance n'est disponible pour les ventilateurs et/ou les blocs d'alimentation du système.
Avertissement concernant un processeur	Un processeur ne fonctionne pas à ses performances ou sa vitesse maximales.
Panne de processeur	Un processeur est en panne.

Tableau 7-1. Événements d'alerte PEF *(suite)*

Évènement	Description
Processeur absent	Un processeur a été supprimé.
PS/VRM/D2D Avertissement	Le bloc d'alimentation, le module de régulation de la tension ou le convertisseur CC à CC va bientôt être en condition de panne.
PS/VRM/D2D Échec	Le bloc d'alimentation, le module de régulation de la tension ou le convertisseur CC à CC est en panne.
Journal du matériel plein ou vide	Un journal du matériel plein ou vide nécessite l'attention de l'administrateur.
Récupération automatique du système	Le système est bloqué ou ne répond pas et effectue une action configurée par la récupération automatique du système.
Avertissement de sonde de puissance système	La consommation d'énergie a presque atteint le seuil de panne.
Panne de sonde de puissance système	La consommation d'énergie a dépassé la limite acceptable la plus élevée et a provoqué une panne.
Flash amovible Média absent	Le média flash amovible est présent.
Flash amovible Panne du média	Le média flash amovible est en attente d'une condition de panne.
Flash amovible Avertissement de média	Le média flash amovible est en attente d'une condition de panne.
État critique de la carte du module SD interne double	Carte du module SD interne double en condition critique.
Carte du module SD interne double en condition d'avertissement	Carte du module SD interne double en condition Panne en attente.
Perte de redondance de la carte du module SD interne double.	La carte du module SD interne double n'a pas de redondance.
Absence de la carte du module SD interne double	La carte du module SD interne double a été retirée.

A

Dépannage

Échec du service de connexion

Sur Red Hat Enterprise Linux, lorsque `SELinux` est défini sur le mode `appliqué`, le service de connexion Dell Systems Management Server Administrator (DSM SA) ne parvient pas à démarrer. Effectuez l'une des étapes suivantes et démarrez ce service :

- Définissez `SELinux` sur le mode `Désactivé` ou sur le mode `Permissif`.
- Modifiez la propriété **allow_execstack** de SELinux pour la définir sur l'état **MARCHE**. Exécutez la commande suivante :

  ```
  setsebool   allow_execstack   on
  ```

- Modifiez le contexte de sécurité du service de connexion DSM 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 l'**avertissement Ignorer le certificat** sur la page d'ouverture de session ;

- les services de Server Administrator ne sont pas activés sur le système VMware ESX/ESXi. Voir le *Guide d'installation de Dell OpenManage Server Administrator*, sur le site **support.dell.com/manuals** pour obtenir des informations sur la façon d'activer les services de Server Administrator sur le système VMware ESX/ESXi.
- le service SFCBD (small footprint CIM broker daemon) du système VMware ESX/ESXi ne s'exécute pas ;
- le service Web Server Management Service du système géré ne s'exécute pas ;
- vous entrez l'adresse IP du système géré et non le nom d'hôte lorsque vous ne cochez pas la case **Ignorer l'avertissement de certificat**.
- la fonctionnalité d'autorisation WinRM (activation distante) n'est pas configurée sur le système géré. Pour des informations sur l'installation de ce logiciel, consultez le *Guide d'installation de Dell OpenManage Server Administrator* disponible à l'adresse **support.dell.com/manuals**.
- Un échec d'authentification se produit lors de la connexion à un système d'exploitation VMware ESXi 4.1/ESX 5.0, pouvant être dû à l'une des raisons suivantes :
  - Le mode `verrouillage` est activé lorsque vous vous connectez au serveur ou lorsque vous avez ouvert une session Server Administrator. Pour plus d'informations sur le mode `verrouillage`, consultez la documentation VMware.
  - Le mot de passe a été modifié alors que votre session Server Administrator est active.
  - Vous ouvrez une session Server Administrator en tant qu'utilisateur ordinaire sans droits d'administrateur. Pour des informations supplémentaires, consultez la documentation VMware relative à l'attribution du rôle.

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

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

Pour forcer une réinstallation :

1. Vérifiez la version de Server Administrator installée précédemment.
2. Depuis **support.dell.com**, téléchargez le progiciel d'installation correspondant à cette version.
3. Localisez **SysMgmt.msi** dans le répertoire **srvadmin\windows\SystemsManagement**.
4. Pour effectuer une réinstallation forcée, tapez la commande suivante à l'invite de commande

   ```
   msiexec /i SysMgmt.msi REINSTALL=ALL
   REINSTALLMODE=vamus
   ```

5. Sélectionnez **Installation personnalisée** et choisissez toutes les fonctionnalités installées à l'origine. Si vous n'êtes pas sûr des fonctionnalités qui ont été installées, sélectionnez toutes les fonctionnalités et effectuez l'installation.

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

6. Lorsque l'application est installée, vous pouvez désinstaller Server Administrator via **Ajout/Suppression de programmes**.

Services OpenManage Server Administrator

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

Tableau A-1. Services OpenManage Server Administrator

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
Windows : DSM SA Connection Service (Service de connexion DSM SA) 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 d'ouvrir une session Server Administrator et d'effectuer une opération quelconque via l'interface utilisateur Web. Néanmoins, la CLI peut toujours être utilisée.	Redémarrer le service	Critique

Tableau A-1. Services OpenManage Server Administrator *(suite)*

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
		Service commun		
Windows : DSM SA Shared Services (Service DSM SA Partagé) 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 Dell System Management Console et Dell IT Assistant (ITA).	Les mises à jour de logiciels ne sont pas possibles via ITA. Toutefois, celles-ci peuvent être exécutées localement et hors de Server Administrator à l'aide des progiciels Dell Update Package. Il est possible d'effectuer des mises à jour à partir d'outils tiers (tels que MSSMS, Altiris et Novell ZENworks).	Redémarrer le service	Avertissement

REMARQUE : Si les bibliothèques de compatibilité 32 bits ne sont pas installées sur un système Linux 64 bits, les services partagés ne parviennent pas à démarrer le collecteur d'inventaire et affichent le message d'erreur `libstdc++.so.5 est requis pour exécuter le Collecteur d'inventaire`. Le RPM srvadmin-cm.rpm fournit les binaires du collecteur d'inventaire. Pour la liste de RPMs dont dépend srvadmin-cm, voir le *Guide d'installation de Dell OpenManage Server Administrator disponible sur le site* support.dell.com/manuals.

Tableau A-1. Services OpenManage Server Administrator *(suite)*

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
Services d'instrumentation				
Windows : DSM SA Data Manager (Gestionnaire de données DSM SA) 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
Gestionnaire d'événements DSM SA (Windows) 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

Tableau A-1. Services OpenManage Server Administrator *(suite)*

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
		Storage Management Service		
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

B

Questions les plus fréquentes

Cette section répertorie les questions les plus fréquentes concernant Dell OpenManage Server Administrator :

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

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

Ce problème provient de la clé de licence autonome (SAL) VMware. Pour en savoir plus, voir l'article de la Base de connaissances sur **kb.vmware.com/kb/1026060**.

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

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

- Ouvrir une session Server Administrator tout en utilisant le système d'exploitation VMware ESX 4.0 U3 et ESX 4.1 U2 en tant que Server Administrator et redémarrer le service de connexion DSM SA.
- Ouvrir une session Remote Node (Nœud à distance) tout en utilisant le système d'exploitation VMware ESX 4.0 U3 and ESX 4.1 U2 en tant Remote Enablement Agent (agent d'activation à distance). Attendre environ 5 minutes afin de permettre au processus sfcbd d'ajouter l'autorisation pour le nouvel utilisateur.

3 **Quel est le niveau d'autorisation minimum nécessaire à un utilisateur pour installer Server Administrator ?**

Vous devez être doté du niveau d'autorisation minimum d'**administrateur** pour pouvoir installer Server Administrator. Les utilisateurs privilégiés et les utilisateurs ne sont pas dotés des autorisations permettant d'installer Server Administrator.

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

Les systèmes dotés de la version 4.3 de Server Administrator doivent être mis à niveau vers la version 6.x puis la version 7.x. Les systèmes dotés d'une version antérieure à 4.3 doivent être d'abord mis à niveau vers la version 4.3, puis vers la version 6.x, et enfin vers la version 7.x (x indique la version de Server Administrator vers laquelle vous souhaitez effectuer une mise à niveau).

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

Connectez-vous à l'adresse : **support.dell.com→ Service informatique→ Manuels→ Logiciels→ Systems Management→ Dell OpenManage Server Administrator**

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

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

Une fois connecté à Server Administrator, naviguez vers **Propriétés→ Résumé**. Vous trouverez la version de Server Administrator installée sur votre système dans la colonne **Systems Management**.

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

Oui, vous pouvez définir votre port https préféré. Naviguez vers **Préférences→ Paramètres généraux→ Web Server→ Port HTTPS**

Au lieu de cliquer sur **Utiliser la valeur par défaut**, cliquez sur **Utiliser le bouton radio pour définir votre port préféré**.

REMARQUE : Si vous donnez un numéro de port qui n'est pas valide ou qui est déjà utilisé, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré. Consultez le Guide d'utilisation : *Installation et sécurité d'OpenManage de Dell* à l'adresse **support.dell.com/manuals** pour une liste complète d'arguments.

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

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

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

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

10 **Le protocole SNMP est-il requis pour la découverte ITA, l'inventaire et les mises à jour de logiciel sur les systèmes PowerEdge ? CIM peut-il être utilisé par lui-même pour la découverte, l'inventaire et les mises à jour ou le protocole SNMP est-il requis ?**

Communication ITA avec les systèmes Linux :

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

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

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 CIM.

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

À l'aide des références de niveau administrateur exigées à la période à laquelle la mise à jour est planifiée ou effectuée, un partage d'administration (lecteur) est établi sur un lecteur du système cible, et une copie de fichier(s) d'un endroit quelconque (éventuellement un autre partage réseau) est effectuée sur le système cible. Les fonctions WMI sont ensuite invoquées 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.

Les périphériques tels que le stockage EMC possèdent des protocoles exclusifs. Certaines informations relatives à cet environnement peuvent être recueillies en consultant les tableaux des ports utilisés dans la documentation OpenManage.

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

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

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

Oui, tout caractère de trait de soulignement dans le nom de domaine est interdit. De plus, tous les autres caractères spéciaux (à l'exception du tiret) sont également interdits. Vous devez utiliser uniquement des lettres majuscules et minuscules, ainsi que des chiffres.

13 Quel est l'impact de l'activation/désactivation 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 disposerez uniquement de l'accès configuré dans Microsoft Active Directory. Vous ne pouvez pas ouvrir de session via la solution Dell Extended Schema Solution dans Microsoft Active Directory. Cette solution vous permet de fournir l'accès à Server Administrator, et d'ajouter et ou/contrôler des utilisateurs et des privilèges de Server Administrator aux utilisateurs existants dans votre logiciel Active Directory. Pour en savoir plus, consultez la section « Utilisation de Microsoft Active Directory » dans le *Guide d'installation de Dell OpenManage Server Administrator* disponible à l'adresse **support.dell.com/manuals**.

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

Pour l'authentification, le contenu des fichiers **/etc/pam.d/openwsman** et **/etc/pam.d/sfcb**, sur le nœud géré, doit être remplacé par :

Pour 32 bits :

```
auth requise pam_stack.so service=system-auth
auth requise /lib/security/pam_nologin.so
compte requis pam_stack.so service=system-auth
```

Pour 64 bits :

```
auth requise pam_stack.so service=system-auth
auth requise /lib64/security/pam_nologin.so
compte requis pam_stack.so service=system-auth
```

Index

D

E

F

O

P

R

S

T

U

V

Z