Dell OpenManage Server Administrator Version 8.5

Guide de l'utilisateur

Novembre 2020
Rév. A01

Remarques, précautions et avertissements

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

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

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

Table des matières

1

Introduction

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

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

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

Sujets :

Installation

Vous pouvez installer Server Administrator à l'aide du *logiciel Dell EMC Systems Management Tools and Documentation*. Le logiciel fournit un programme de configuration pour installer, mettre à niveau ou désinstaller les composants logiciels de Server Administrator, du système géré et de la station de gestion. En outre, vous pouvez installer Server Administrator sur plusieurs systèmes via une installation sans assistance sur un réseau. Le programme d'installation de Server Administrator fournit des scripts d'installation et des progiciels RPM pour installer et désinstaller Server Administrator et d'autres composants logiciels de système géré sur votre système géré. Pour en savoir plus, consultez le *Guide d'installation de Server Administrator* et le *Guide d'installation du logiciel de la station de gestion* à l'adresse **dell.com/opemanagemanuals**.

REMARQUE : lorsque vous installez les progiciels « open source » depuis le logiciel *Dell EMC Systems Management Tools and Documentation*, les fichiers de licence correspondants sont automatiquement copiés sur le système. Lorsque vous supprimez ces progiciels, les fichiers correspondants sont également supprimés.

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

Mise à jour de composants système particuliers

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

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

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

Storage Management Service (Service de gestion de stockage)

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

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

Instrumentation Service

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

Contrôleur d'accès à distance (RAC)

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

Journaux

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

Nouveautés de cette version

Les points les plus intéressants d'OpenManage Server Administrator sont les suivants :

- Prise en charge des systèmes d'exploitation suivants :
  - VMware ESXi 6.5
  - VMware ESXi 6.0 U3
  - Microsoft Windows Server 2016

    REMARQUE : La prise en charge du système d'exploitation Citrix XenServer a été supprimée pour Server Administrator et Storage Management.
- Prise en charge des navigateurs suivants :
  - Internet Explorer - 9, 10, 11
  - Microsoft Edge 25
  - Google Chrome - 54
  - Safari - 9.x
  - Mozilla Firefox - 50, 51

REMARQUE : La plateforme PowerEdge C6320P n'est pas prise en charge pour Server Administrator Storage Management 8.5

- Prise en charge de Java Runtime Environment 8 mise à jour 112.
- Prise en charge de carte SD 32 Go et 64 Go.

REMARQUE : La plateforme C6320P n'est pas prise en charge pour OpenManage Server Administrator 8.5.

REMARQUE : Pour consulter la liste des systèmes d'exploitation et des serveurs Dell pris en charge, voir la *Matrice de prise de prise en charge logicielle des systèmes Dell* dans la version requise du **logiciel OpenManage** sur **dell.com/openmanagemanuals**.

Disponibilité des normes de gestion des systèmes

Server Administrator prend en charge les protocoles de gestion de systèmes suivants :

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

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

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

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

Disponibilité sur les systèmes d'exploitation pris en charge

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

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

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

Tableau 1. Disponibilité des normes de Systems Management

Système d'exploitation	SNMP	CIM
Famille Windows Servers 2008	Disponible sur le média d'installation du système d'exploitation	Toujours installé
Red Hat Enterprise Linux	Disponible dans le progiciel net-snmp du média d'installation du système d'exploitation	Non disponible
SUSE Linux Enterprise Server	Disponible dans le progiciel net-snmp du média d'installation du système d'exploitation	Non disponible
VMWare 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

Page d'accueil de Server Administrator

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

Autres documents utiles

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

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

- Consultez le *Dell OpenManage Server Update Utility User's Guide* (Guide d'utilisation de l'utilitaire Dell OpenManage Server Update Utility) pour plus d'informations sur la manière d'obtenir et d'utiliser Server Update Utility (SUU) pour mettre à jour vos systèmes Dell ou pour afficher les mises à jour disponibles pour n'importe quel système répertorié dans l'espace de stockage.
- Le *Dell Management Console User's Guide* (Guide d'utilisation de Dell Management Console) fournit des informations sur l'installation, la configuration et l'utilisation de Dell Management Console.
- Le *Dell Lifecycle Controller User's Guide* (Guide d'utilisation de Dell Life Cycle Controller) fournit des informations sur la configuration et l'utilisation d'Unified Server Configurator pour effectuer des tâches de gestion de systèmes et de stockage tout au long du cycle de vie de votre système.
- Le *Dell License Manager User's Guide* (Guide d'utilisation de Dell License Manager) fournit des informations sur la gestion des licences de serveur de composant pour serveurs Dell 12G.
- Le *Glossaire* offre des informations sur la terminologie utilisée dans le présent document.

Accès au contenu de support à partir du site de support Dell EMC

Accédez au contenu de support lié à un ensemble d'outils de gestion de systèmes à l'aide de liens directs, en accédant au site de support Dell EMC, ou à l'aide d'un moteur de recherche.

- Liens directs :
  - Pour la gestion des systèmes Dell EMC Enterprise et la gestion à distance des systèmes Dell EMC Enterprise à distance :https://www.dell.com/esmmanuals
  - Pour les solutions de virtualisation Dell EMC :https://www.dell.com/SoftwareManuals
  - Pour Dell EMC OpenManage :https://www.dell.com/openmanagemanuals
  - Pour iDRAC :https://www.dell.com/idracmanuals
  - Pour la gestion des systèmes Dell EMC OpenManage Connections Enterprise :https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Pour les outils facilitant la maintenance Dell EMC :https://www.dell.com/serviceabilitytools
- Site de support Dell EMC :
  1. Rendez-vous sur https://www.dell.com/support.
  2. Cliquez sur **Parcourir tous les produits**.
  3. Sur la page **Tous les produits**, cliquez sur **Logiciel** et cliquez sur le lien requis.
  4. Cliquez sur le produit requis, puis sur la version requise.

À l'aide des moteurs de recherche, saisissez le nom et la version du document dans la zone de recherche.

Obtention d'une assistance technique

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

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

Contacter Dell EMC

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

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

Rendez-vous sur **Dell.com/contactdell.**

2

Configuration et administration

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

Sujets :

Contrôle des accès basé sur des rôles

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

Privilèges utilisateur

Server Administrator offre différents droits d'accès en fonction des privilèges de groupe attribués à l'utilisateur. Quatre niveaux de privilège utilisateur existent : utilisateur, utilisateur privilégié, administrateur et administrateur élevé.

Tableau 2. Privilèges utilisateur

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

Niveaux de privilèges pour accéder aux services de Server Administrator

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

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

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

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

Authentification

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

Authentification de Microsoft Windows

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

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

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

Authentification de VMware ESXi Server 5.X

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

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

Cryptage

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

Attribution des privilèges d'utilisateur

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

PRÉCAUTION : Pour protéger l'accès aux composants critiques de votre système, vous devez attribuer un mot de passe à chaque compte d'utilisateur ayant accès au logiciel Dell OpenManage.

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

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

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

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

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

1. Accédez à **Panneau de configuration** > **Outils d'administration** > **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, effectuez un clic droit sur **Utilisateurs** ou sur le conteneur auquel vous voulez ajouter le nouvel utilisateur et pointez sur **Nouveau** > **Utilisateur**.
3. Tapez les informations appropriées concernant le nom d'utilisateur dans la boîte de dialogue et cliquez sur **Next** (Suivant).
4. Cliquez sur **Next** (Suivant), puis sur **Finish** (Terminer).
5. Double-cliquez sur l'icône représentant l'utilisateur que vous avez créé.
6. Cliquez sur l'onglet **Member of** (Membre de).
7. Cliquez sur **Ajouter**.
8. Sélectionnez le groupe approprié puis cliquez sur **Add** (Ajouter).
9. Cliquez sur **OK**, puis cliquez de nouveau sur **OK**.

   REMARQUE : Les nouveaux utilisateurs peuvent ouvrir une session dans 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 racine. Pour plus d'informations sur la création d'utilisateurs et de groupes d'utilisateurs, consultez la documentation de votre système d'exploitation.

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

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

Liens associés :

- Création d'utilisateurs avec des privilèges d'utilisateur
- Création d'utilisateurs avec des privilèges d'utilisateur privilégié

Création d'utilisateurs avec des privilèges d'utilisateur

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

   REMARQUE : Si `<group>` n'existe pas, vous devez le créer à l'aide de la commande **groupadd**.

2. Tapez `passwd <nom_d'utilisateur>` et appuyez sur <Entrée>.
3. Lorsque vous y êtes invité, entrez un mot de passe pour le nouvel utilisateur.

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

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

Création d'utilisateurs avec des privilèges d'utilisateur privilégié

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

   REMARQUE : Définissez `root` en tant que groupe principal.

2. Tapez `passwd <nom_d'utilisateur>` et appuyez sur <Entrée>.
3. Lorsque vous y êtes invité, entrez un mot de passe pour le nouvel utilisateur.

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

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

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

REMARQUE : Vous devez être connecté en tant qu'utilisateur racine ou équivalent.

1. Ouvrez le fichier **omarolemap** qui se trouve dans `/opt/dell/srvadmin/etc/omarolemap`.
2. Ajoutez ce qui suit au fichier : `<User_Name>[Tab]<Host_Name>[Tab]<Rights>`

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

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

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

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

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

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

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

<Nom_d'utilisateur>	<Nom_d'hôte>	<Droits>
Mike	192.168.2.3	Utilisateur privilégié

3. Enregistrez et fermez le fichier.

Meilleures pratiques lors de l'utilisation du fichier omarolemap

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

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

Tableau 6. Meilleures pratiques en matière de fichier omarolemap

root	Administrateur
+root	* Poweruser (utilisateur avancé racine)
*	* User (Utilisateur racine)

- Ne modifiez pas les permissions ou le format du fichier **omarolemap.**
- N'utilisez pas l'adresse de retour de boucle pour <*Host_Name*>, par exemple : localhost ou 127.0.0.1.
- Lorsque les services de connexion ont été redémarrés et que les modifications ne sont pas effectives pour le fichier **omarolemap**, consultez le journal des commandes pour prendre connaissance des erreurs.
- Lorsque le fichier **omarolemap** est copié d'un ordinateur à un autre, les permissions et les entrées du fichier doivent être revérifiées.
- Précédez le *Group Name* du signe *+*.
- Server Administrator utilise les privilèges utilisateur par défaut du système d'exploitation si :
  - un utilisateur est dégradé dans le fichier **omarolemap**
  - des saisies en double de noms d'utilisateurs ou de groupes d'utilisateurs existent et présentent le même <*Host_Name*>
- Vous pouvez également utiliser `Space` pour délimiter les colonnes au lieu de `[Tab]`.

Création d'utilisateurs Server Administrator pour VMware ESXi 5.*X* et ESXi 6.*X*

Pour ajouter un utilisateur au tableau répertoriant les utilisateurs :

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

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

REMARQUE : Vous devez être connecté avec des privilèges d'administrateur.

1. Ouvrez la fenêtre **Gestion de l'ordinateur**.
2. Dans l'arborescence de la console, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Utilisateurs**.
3. Double-cliquez sur le compte d'utilisateur dénommé **Invité** ou **système_IUSR** pour afficher les propriétés de ces utilisateurs, ou effectuez un clic droit sur le compte d'utilisateur dénommé **Invité** ou **IUSR_***nom du système*, 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 le protocole SMNP (protocole de gestion de réseau simple), un protocole de gestion des systèmes standard, sur tous les systèmes d'exploitation pris en charge. La prise en charge SNMP peut être installée ou non selon le système d'exploitation dont vous disposez et la façon dont celui-ci a été installé. Dans la plupart des cas, SNMP est installé lors de l'installation de votre système d'exploitation. Un protocole de gestion des systèmes standard installé et pris en charge, tel que SNMP, est nécessaire à l'installation de Server Administrator.

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

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

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

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

- Configuration de l'agent SNMP pour les systèmes exécutant des systèmes d'exploitation Windows pris en charge
- Configuration de l'agent SNMP sur les systèmes fonctionnant sous un système d'exploitation Red Hat Enterprise Linux pris en charge
- Configuration de l'agent SNMP sur les systèmes fonctionnant sous des systèmes d'exploitation SUSE Linux Enterprise Server pris en charge
- Configuration de l'agent SNMP sur des systèmes exécutant les systèmes d'exploitation VMware ESXi 5.X et ESXi 6.X pris en charge

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

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

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

Modification du nom de communauté SNMP

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

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

1. Ouvrez la fenêtre **Computer Management** (Gestion de l'ordinateur).
2. Développez l'icône **Computer Management** dans la fenêtre, si nécessaire.
3. Développez l'icône **Services and Applications** (Services et applications) et cliquez sur **Services**.

4. Faites défiler la liste des services jusqu'à ce que vous trouviez **SNMP Service** (Service SNMP), effectuez un clic droit sur **SNMP Service**, puis cliquez sur **Properties** (Propriétés).

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

   Pour ajouter un nom de communauté :

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

      La fenêtre de **SNMP Service Configuration** (Configuration du Service SNMP) s'affiche.
   b. Saisissez le nom de communauté d'un système qui peut gérer votre système (public par défaut) dans la zone de texte **Nom de communauté** et cliquez sur **Add** (Ajouter).

      La fenêtre des **Propriétés du Service SNMP** s'affiche.

   Pour modifier un nom de communauté :

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

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

      La fenêtre des **SNMP Service Properties** (Propriétés du Service SNMP) s'affiche.
6. Cliquez sur **OK** pour enregistrer les modifications.

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

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

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

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

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

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

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

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

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

Configuration du contrôle d'accès de l'agent SNMP

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

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

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

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

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

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

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

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Modification du nom de communauté SNMP

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

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

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

   REMARQUE : Pour IPv6, trouvez la ligne `com2sec6 notConfigUser default public`. Ajoutez également le texte suivant au fichier : `agentaddress udp6:161`.

3. Modifiez cette ligne en remplaçant `public` par le nouveau nom de communauté SNMP. Une fois modifiée, la nouvelle ligne devrait être comme suit : `com2sec publicsec default community_name` ou `com2sec notConfigUser default community_name`.
4. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant `service snmpd restart`.

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

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

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

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

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

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

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

Actions d'installation SNMP de Server Administrator

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

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

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

La configuration par défaut de l'agent SNMP sur les systèmes d'exploitation SUSE Linux Enterprise Server fournit un accès en lecture seule à l'intégralité de l'arborescence MIB (base d'information de gestion) de la communauté « public » depuis l'hôte local uniquement. Cette configuration ne permet pas aux applications de gestion SNMP telles qu'IT Assistant de s'exécuter sur d'autres hôtes pour découvrir et gérer correctement les systèmes Server Administrator. Si Server Administrator détecte cette configuration pendant l'installation, il enregistre un message dans le fichier journal du système d'exploitation, `/var/log/messages`, pour indiquer que l'accès SNMP est limité à l'hôte local. Vous devez configurer l'agent SNMP pour activer l'accès SNMP à partir d'hôtes distants si vous comptez gérer le système à l'aide d'applications de gestion SNMP d'hôtes distants.

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

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

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

   REMARQUE : Vous pouvez activer l'accès SNMP à partir de plusieurs hôtes distants spécifiques en ajoutant une directive `rocommunity` pour chaque hôte distant.

3. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : `/etc/init.d/snmpd restart`.

   Pour activer l'accès SNMP à partir de tous les hôtes distants à un système exécutant Server Administrator, modifiez le fichier de configuration de l'agent SNMP (`/etc/snmp/snmpd.conf`) et effectuez les étapes suivantes :

4. Trouvez la ligne `rocommunity public 127.0.0.1`.

5. Modifiez cette ligne en supprimant 127.0.0.1. Une fois modifiée, la nouvelle ligne devrait être comme suit : `rocommunity public`.
6. Pour activer les modifications de la configuration SNMP, redémarrez l'agent SNMP en tapant : `/etc/init.d/snmpd restart`.

Modification du nom de communauté SNMP

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

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

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

Configuration de l'agent SNMP sur des systèmes exécutant les systèmes d'exploitation VMware ESXi 5.X et ESXi 6.X pris en charge

Server Administrator prend en charge les interruptions SNMP sur VMware ESXi 5.X et ESXi 6.X. Si seule une licence autonome est présente, la configuration SNMP échoue sur les systèmes d'exploitation VMware ESXi. Server Administrator ne prend pas en charge les opérations Get et Set SNMP sur VMWare ESXi 5.X et ESXi 6.X, car la prise en charge SNMP requise n'est pas disponible. L'interface de ligne de commande (CLI) VMware vSphere sert à configurer les systèmes exécutant VMware ESXi 5.X et ESXi 6.X pour qu'ils envoient des interruptions SNMP à la station de gestion.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Le menu **Choose a Tool** (Choisir un outil) apparaît.
2. Sélectionnez **Firewall Configuration** (Configuration du pare-feu) en utilisant la flèche vers le bas et appuyez sur <Entrée>. L'écran **Firewall Configuration** apparaît.
3. Appuyez sur <Tab> pour sélectionner **Security Level** (Niveau de sécurité), puis appuyez sur la barre d'espace pour sélectionner le niveau de sécurité que vous souhaitez configurer. Le **Security Level** (Niveau de sécurité) sélectionné est indiqué par un astérisque.

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

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

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

Configuration du pare-feu

Pour ouvrir le port SNMP sur SUSE Linux Enterprise Server :

1. Configurez SuSEfirewall2 en exécutant la commande suivante sur une console :`a.# yast2 firewall`
2. Utilisez les touches fléchées pour accéder à **Services autorisés**.
3. Appuyez sur <Alt><d> pour ouvrir la boîte de dialogue **Ports autorisés supplémentaires**.
4. Appuyez sur <Alt><T> pour déplacer le curseur dans la zone de texte **Ports TCP**.
5. Saisissez **snmp** dans la zone de texte.

6. Appuyez sur <Alt><O> <Alt><N> pour passer à l'écran suivant.
7. Appuyez sur <Alt><A> pour accepter et appliquer les modifications.

3

Utilisation de Server Administrator

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

L'écran **Server Administrator Log in** (Ouverture de session Server Administrator) s'affiche. Le port par défaut pour Server Administrator est 1311. Vous pouvez modifier le port si nécessaire. Pour des instructions sur la configuration de vos préférences système, voir Dell Systems Management Server Administration Connection Service and Security Setup (Service de connexion à l'administration du serveur de gestion des systèmes Dell et configuration de la sécurité).

REMARQUE : Les serveurs s'exécutant sur XenServer 6.5 peuvent être gérés à l'aide de l'interface CLI ou d'un serveur Web central installé sur un système séparé.

Sujets :

Ouverture et fermeture de session

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

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

Ouverture d'une session Server Administrator sur le système local

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

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

Pour ouvrir une session Server Administrator sur un système local :

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

   Si vous accédez à Server Administrator à partir d'un domaine défini, vous devez également spécifier le nom de domaine approprié.

2. Sélectionnez l'option **Ouverture de session Active Directory** pour vous connecter avec Microsoft Active Directory. Voir Utilisation de l'ouverture de session Active Directory.
3. Cliquez sur **Envoyer**.

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

REMARQUE : Pour en savoir plus sur la configuration d'Active Directory sur les systèmes utilisant la CLI, voir le *Guide d'installation du logiciel Management Station* à l'adresse `dell.com/openmanagemanuals`.

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

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

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

   REMARQUE : Si vous avez fourni le nom du système ou le nom de domaine complet (FQDN), l'hôte de Server Administrator Web Server convertit le nom du système ou le nom de domaine complet (FQDN) pour l'adresse IP du système géré. Vous pouvez également vous connecter en fournissant le numéro de port du système géré dans le format suivant : Nom d'hôte : Numéro de port ou Adresse IP : Numéro de port. Si vous vous connectez à un serveur Citrix XenServer, Server Administrator Web Server sélectionne automatiquement le port par défaut (5986) ou vous pouvez spécifier un autre port.

3. Si vous utilisez une connexion Intranet, sélectionnez **Ignore Certificate Warnings** (Ignorer les avertissements de certificat).
4. Sélectionnez **Active Directory Login** (Ouverture de session Active Directory) pour vous connecter avec l'authentification Microsoft Active Directory. Si le logiciel Active Directory ne sert pas à contrôler l'accès à votre réseau, ne sélectionnez pas **Active Directory Login**. Voir Utilisation de la connexion Active Directory.
5. Cliquez sur **Submit** (Soumettre).

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

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

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

   REMARQUE : Assurez-vous de bien saisir `https://` (et non `http://`) dans le champ d'adresse.

3. Appuyez sur <Entrée>.

Ouverture d'une session Central Web Server

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

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

   PRÉCAUTION : L'écran d'ouverture de session affiche une case à cocher Ignorer les avertissements de certificat. Nous vous recommandons d'utiliser cette option avec discrétion et de ne l'utiliser que dans des environnements Intranet de confiance.

2. Cliquez sur le lien **Manage Web Server** (Gérer Web Server) qui se trouve dans le coin supérieur droit de l'écran.
3. Entrez les **User Name, Password** (Nom d'utilisateur, mot de passe) et **Domain Name** (Nom de domaine) (si vous accédez à Server Administrator à partir d'un domaine défini), puis cliquez sur **Submit** (Soumettre).
4. Sélectionnez **Ouverture de session Active Directory** pour vous connecter avec Microsoft Active Directory. Voir Utilisation de l'ouverture de session Active Directory.
5. Cliquez sur **Submit** (Soumettre).

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

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

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

REMARQUE : Si l'autorité de certification du système géré est valide et si le serveur web Server Administrator signale encore une erreur de certificat non fiable, vous pouvez tout de même en faire une autorité de certification de confiance à l'aide du fichier `certutil.exe`. Pour en savoir plus sur l'accès à ce fichier .exe, voir la documentation de votre système d'exploitation. Sur les systèmes d'exploitation Windows pris en charge, vous pouvez également utiliser l'option d'alignement des certificats pour importer des certificats.

Utilisation de l'ouverture de session Active Directory

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

Cette solution vous permet de donner l'accès à Server Administrator, ce qui signifie qu'elle vous permet d'ajouter/contrôler les utilisateurs de Server Administrator et les privilèges des utilisateurs existants dans votre logiciel Active Directory. Pour en savoir plus, voir la section « Utilisation de Microsoft Active Directory » du document *Guide d'installation de Server Administrator* à l'adresse `dell.com/openmanagemanuals`.

Connexion directe

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

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

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

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

où `plugin name = omsa, ita,` etc.

Par exemple :

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

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

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

où `plugin name = omsa, ita,` etc.

Par exemple :

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

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

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

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

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

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

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

1. Dans votre navigateur Web, cliquez sur **Outils** > **Options Internet** > **Sécurité**.
   La fenêtre **Internet Options** s'affiche.
2. Sous **Sélectionner une zone pour afficher ou modifier les paramètres de sécurité**, cliquez sur **Sites de confiance** puis sur **Sites**.
3. Dans le champ **Ajouter ce site Web à la zone**, collez l'adresse Web utilisée pour accéder au système géré distant.
4. Cliquez sur **Ajouter**.
5. Copiez l'adresse Web utilisée pour accéder au système géré distant depuis la barre d'adresse du navigateur et collez-la dans le champ **Ajouter ce site Web à la zone**.
6. Sous **Niveau de sécurité pour cette zone**, cliquez sur **Personnaliser le niveau**.
7. Cliquez sur **OK** pour enregistrer les nouveaux paramètres.
8. Fermez le navigateur et ouvrez une session Server Administrator.

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

Pour autoriser l'authentification unique (SSO) pour Server Administrator sans demander la saisie d'informations d'identification de l'utilisateur :

1. Dans votre navigateur Web, cliquez sur **Outils** > **Options Internet** > **Sécurité**
2. Sous **Sélectionner une zone pour afficher ou modifier les paramètres de sécurité**, cliquez sur **Sites de confiance** puis sur **Sites**.
3. Dans le champ **Ajouter ce site Web à la zone**, collez l'adresse Web utilisée pour accéder au système géré distant.
4. Cliquez sur **Ajouter**.
5. Cliquez sur **Niveau personnalisé**.
6. Sous **Authentification de l'utilisateur**, sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuels**.
7. Cliquez sur **OK** pour enregistrer les nouveaux paramètres.
8. Fermez le navigateur et ouvrez une session Server Administrator.

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

1. Ouvrez votre navigateur.
2. Cliquez sur **Modifier** > **Préférences**.
3. Sélectionnez **Avancé** > **Scripts et Plug-ins**.
4. Sous Activer JavaScript pour, assurez-vous que Navigateur est sélectionné. Assurez-vous que la case à cocher **Navigateur** est cochée sous **Activer JavaScript pour**.
5. Cliquez sur **OK** pour enregistrer les nouveaux paramètres.
6. Fermez le navigateur.
7. Ouvrez une session sur Server Administrator.

Page d'accueil de Server Administrator

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

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

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

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

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

Tableau 7. Noms des champs de l'interface utilisateur graphique et systèmes applicables

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

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

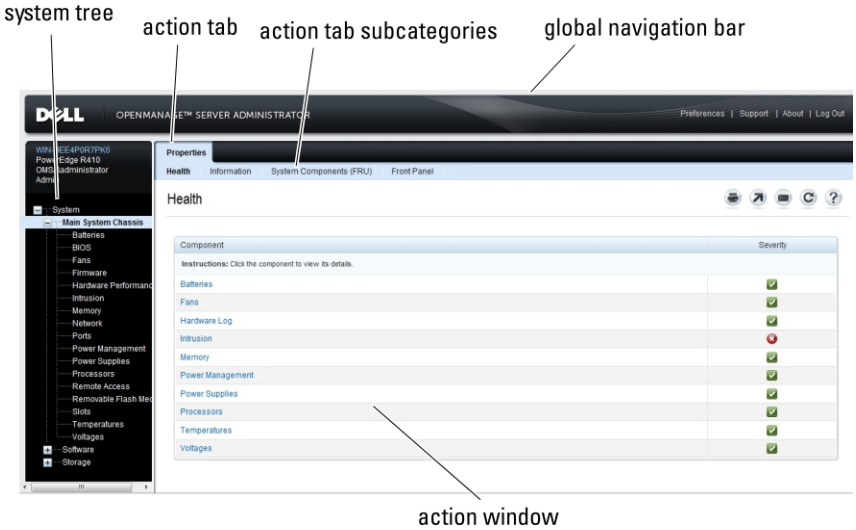

Figure 1. Exemple de page d'accueil de Server Administrator — Système non modulaire

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

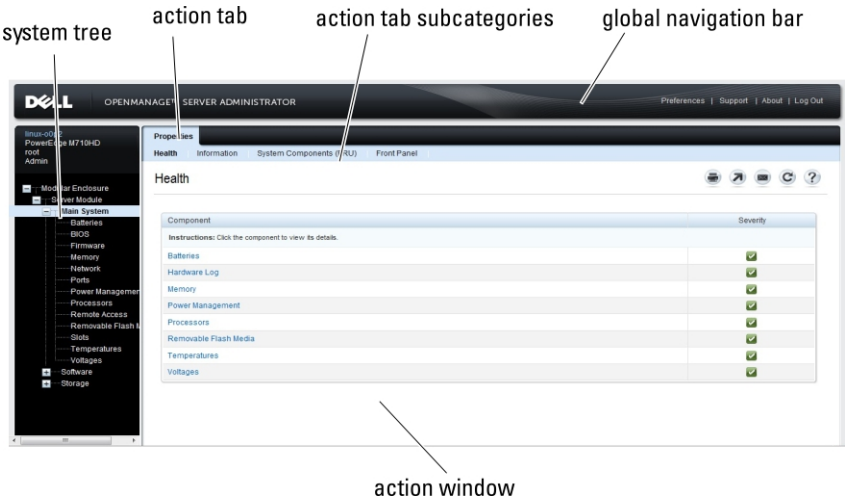

Figure 2. Exemple de page d'accueil de Server Administrator — Système modulaire

Si vous cliquez sur un objet dans l'arborescence système, une fenêtre d'action correspondante à cet objet s'ouvre. Vous pouvez naviguer dans la fenêtre d'actions en cliquant sur les onglets d'actions pour sélectionner les catégories principales et en cliquant sur les sous-catégories de l'onglet d'actions pour accéder à des informations plus détaillées ou des actions plus ciblées. Les informations affichées dans la zone de données de la fenêtre d'actions peuvent aller des journaux système aux voyants d'état et jauges du capteur système. Les éléments soulignés dans la zone de données de la fenêtre d'actions indiquent un niveau de fonctionnalité plus important. Si vous cliquez sur un élément souligné, une zone de données contenant plus de détails se crée dans la fenêtre d'actions. Par exemple, si vous cliquez sur **Châssis du système principal/système principal** dans la sous-catégorie **Intégrité** de l'onglet d'actions **Propriétés**, l'état d'intégrité de tous les composants contenus dans l'objet châssis du système principal/système principal dont l'état d'intégrité est surveillé est répertorié.

REMARQUE : Des privilèges d'administrateur ou d'utilisateur privilégié sont requis pour afficher la plupart des objets de l'arborescence système, des composants système, des onglets d'actions et des fonctionnalités des zones de données configurables. En outre, seuls les utilisateurs connectés avec des privilèges d'administrateur ont accès aux fonctionnalités système critiques, telles que la fonctionnalité d'arrêt disponible dans l'onglet **Arrêt**.

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

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

Tableau 8. Différences d'interface utilisateur de Server Administrator au sein des systèmes modulaires et non modulaires

Fonctions	Système modulaire	Système non-modulaire
Batteries	✓	✓
Blocs d'alimentation	✗	✓
Ventilateurs	✗	✓
Hardware Performance	✗	✓
Intrusion	✗	✓
Mémoire	✓	✓
Réseau	✓	✓

Tableau 8. Différences d'interface utilisateur de Server Administrator au sein des systèmes modulaires et non modulaires (suite)

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

Barre de navigation globale

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

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

Arborescence système

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

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

Fenêtre d'action

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

En cliquant sur un objet dans l'arborescence du système, vous ouvrez la fenêtre d'actions de ce composant, ce qui affiche tous les onglets Action disponibles. La zone de données affiche par défaut une sous-catégorie présélectionnée du premier onglet d'action correspondant à l'objet sélectionné.

La sous-catégorie présélectionnée correspond généralement à la première option. Par exemple, en cliquant sur l'objet **Châssis principal du système/système principal**, vous ouvrez une fenêtre d'actions dans laquelle l'onglet d'action **Propriétés** et la sous-catégorie **Intégrité** s'affiche dans la zone de données de la fenêtre.

Zone de données

La zone de données se trouve sous les onglets d'action sur le côté droit de la page d'accueil. La zone de données est l'emplacement où vous effectuez des tâches ou affichez des détails sur les composants système. Le contenu de la fenêtre dépend de l'objet de l'arborescence système et de l'onglet d'action qui est actuellement sélectionné. Par exemple, lorsque vous sélectionnez **BIOS** dans l'arborescence système, l'onglet **Propriétés** est sélectionné par défaut et les informations sur la version du BIOS du système s'affichent dans la zone de données. La zone de données de la fenêtre d'action contient de nombreuses fonctionnalités communes, notamment les indicateurs d'état, les boutons de tâche, les éléments soulignés et les indicateurs de niveau.

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

Indicateurs de condition des composants de système/module de serveur

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

Tableau 9. Indicateurs de condition des composants de système/module de serveur

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

Boutons de tâches

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

- Si vous cliquez sur **Imprimer** ( ), une copie de la fenêtre ouverte s'imprime sur votre imprimante par défaut.
- En cliquant sur **Exporter** ( ), vous générez un fichier texte qui répertorie les valeurs de chaque champ de données sur la fenêtre ouverte. Le fichier d'exportation est enregistré à l'emplacement que vous spécifiez. Pour plus d'informations sur la personnalisation du délimiteur qui sépare les valeurs de champ de données, consultez les sections « Configuration utilisateur » et « Préférences système ».
- En cliquant sur **E-mail** ( ), vous créez un e-mail adressé à votre destinataire. Pour obtenir des instructions sur la configuration du serveur de messagerie et du destinataire de l'e-mail par défaut, reportez-vous aux sections « Configuration utilisateur » et « Préférences système ».
- 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 **Save As**, un fichier HTML de la fenêtre d'action est enregistré dans un fichier **.zip**.
- Si vous cliquez sur **Clear Log**, tous les événements du journal affichés dans la zone de données de la fenêtre d'action sont supprimés.
- Si vous cliquez sur **Aide** ( ), des informations détaillées concernant la fenêtre spécifique ou le bouton de tâche affiché apparaissent.

REMARQUE : Les boutons **Exporter**, **E-mail** et **Enregistrer sous** ne sont visibles que pour les utilisateurs connectés avec des droits d'utilisateur privilégié ou des privilèges d'administration. Le bouton **Effacer le journal** est visible uniquement pour les utilisateurs disposant de privilèges d'administration.

Éléments soulignés

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

Indicateurs de niveau

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

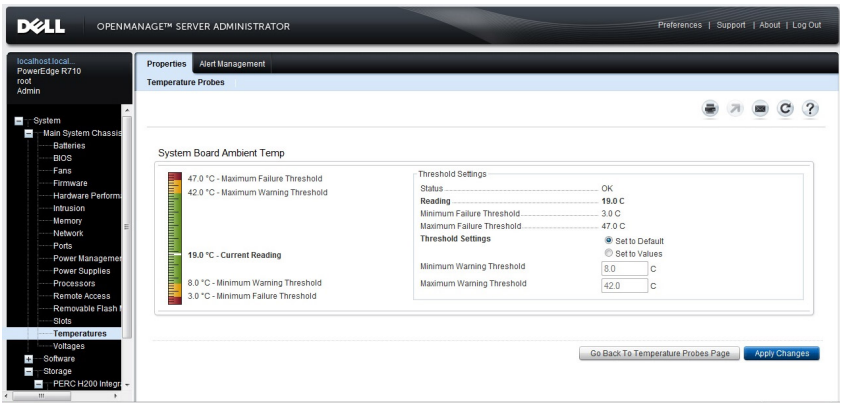

Figure 3. Indicateur de niveau

Utilisation de l'aide en ligne

Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. Cliquez sur **Aide** pour ouvrir une fenêtre indépendante contenant des informations détaillées sur la fenêtre spécifique que vous visualisez. L'aide en ligne est conçue pour vous guider tout au long des actions spécifiques nécessaires à l'exécution de tous les aspects des services Server Administrator. L'aide en ligne est disponible pour toutes les fenêtres que vous pouvez afficher, en fonction des groupes de logiciels et de matériel détectés par Server Administrator sur le système et du niveau de privilèges de l'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** lorsque vous vous connectez pour gérer un système distant. Cet onglet est également disponible lorsque vous vous connectez pour gérer le serveur Web Server Administrator ou le système local.

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

- La barre de navigation globale, qui fournit des liens vers des services généraux.
  - Cliquez sur **Accueil** pour revenir à la page d'accueil de Server Administrator.
- Le panneau gauche de la page d'accueil **Preferences** (là où s'affiche l'arborescence du système sur la page d'accueil de Server Administrator) affiche les différentes catégories de préférences du système géré ou Server Administrator Web Server.
- La fenêtre d'action affiche les paramètres disponibles et les préférences du système géré ou de Server Administrator Web Server.

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

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

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

  REMARQUE : Les formats possibles sont les suivants : **traditional** (traditionnel) et **enhanced** (optimisé). Le format par défaut est **traditional**, le format hérité.
- Active la sauvegarde automatique et l'effacement des entrées du journal ESM.

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

  La sauvegarde est enregistrée sur :

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

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

  REMARQUE : Cette fonction n'est disponible que sur les systèmes Dell PowerEdge de 10e et 11e générations. L'iDRAC fournit une sauvegarde automatique et la fonctionnalité de suppression du journal SEL sur les serveurs PowerEdge de 12e génération et générations ultérieures.
- Sélectionnez ou désélectionnez les gravités des entrées du journal saisies dans le journal des événements principaux du système d'exploitation. Sélectionnez les valeurs possibles : **Critique**, **Avertissement du journal** ou **Information du journal**

  REMARQUE : Toutes les options sont sélectionnées par défaut. La fonction de filtre de journalisation du système d'exploitation est disponible lorsque le composant filtre de journalisation du système d'exploitation est installé.
- Sélectionnez **Activer** pour consigner tous les événements de capteurs ESM non surveillés. Par l'activation de cette fonction, Server Administrator génère des interruptions SNMP, des journaux de système d'exploitation et des alertes pour tous les capteurs non surveillés.
- Configurer la taille du journal des commandes
- Configurer le protocole SNMP

Préférences de Server Administrator Web Server

Lorsque vous ouvrez une session sur le serveur Server Administrator Web, la page d'accueil Préférences revient par défaut à la fenêtre Préférences utilisateur sous l'onglet **Préférences**.

En fonction de la séparation du serveur Server Administrator Web à partir du système géré, les options suivantes s'affichent lorsque vous vous connectez au serveur Server Administrator Web à l'aide du lien Manage Web Server :

- Préférences du serveur Web
- Gestion du certificat X.509

Pour plus d'informations sur l'accès à ces fonctionnalités, consultez la section Présentation des 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 Webserver.

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

Pour définir vos préférences utilisateur :

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

   La page d'accueil **Préférences** s'affiche.
2. Cliquez sur **Paramètres généraux**.
3. Pour ajouter un destinataire de courrier électronique/e-mail pré-sélectionné, saisissez l'adresse e-mail de votre contact désigné pour le service dans le champ **Destinataire**, puis cliquez sur **Appliquer**.

   REMARQUE : Cliquez sur **E-mail** () dans une fenêtre pour envoyer un e-mail avec, en pièce jointe, un fichier HTML de la fenêtre à l'adresse e-mail désignée.

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

Préférences Webserver

Procédez comme suit pour configurer vos préférences Webserver :

1. Cliquez sur **Preferences** (Préférences) sur la barre de navigation globale.

   La page d'accueil **Preferences** (Préférences) apparaît.
2. Cliquez sur **General Settings** (Paramètres généraux).
3. Dans la fenêtre **Préférences serveur**, définissez les options souhaitées.
   - Utilisez la fonction **Délai d'expiration de la session (en minutes)** pour définir la durée limite pendant laquelle une session Server Administrator reste active. Sélectionnez **Activer** pour autoriser Server Administrator à expirer si aucune interaction utilisateur ne survient pendant une durée spécifiée (en minutes). Les utilisateurs dont la session expire doivent se reconnecter pour continuer. Sélectionnez **Désactiver** si vous souhaitez désactiver la fonction **Délai d'expiration de la session (en minutes)** de Server Administrator.
   - Le champ **Port HTTPS** indique le port sécurisé de Server Administrator. Le port sécurisé par défaut pour Server Administrator est 1311.

     REMARQUE : Si vous modifiez le numéro de port en le remplaçant par un numéro non valide ou déjà utilisé, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré. Pour obtenir la liste des ports par défaut, consultez le *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse **dell.com/openmanagemanuals**.
   - Le champ **Adresse IP à lier à** indique la ou les adresses IP du système géré auxquelles Server Administrator est lié au démarrage d'une session. Sélectionnez **Toutes** pour lier toutes les adresses IP applicables de votre système. Sélectionnez **Spécifique** pour relier une adresse IP spécifique.

     REMARQUE : Si vous donnez une autre valeur que **All** (Toutes) au champ **IP Address to Bind**, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré.
   - Le champ **Destinataire** spécifie la ou les adresses auxquelles vous souhaitez envoyer des e-mails concernant les mises à jour par défaut. Vous pouvez configurer plusieurs adresses e-mail en les séparant par une virgule.
   - Les champs **Nom du serveur SMTP (ou adresse IP)** et **Suffixe DNS du serveur SMTP** spécifient le protocole SMTP et le suffixe DNS (serveur de noms de domaine) de votre entreprise ou organisation. Pour permettre à Server Administrator d'envoyer des e-mails, vous devez saisir les adresses IP et le suffixe DNS du serveur SMTP de votre entreprise ou organisation dans les champs appropriés.

     REMARQUE : Pour des raisons de sécurité, votre entreprise ou organisation peut interdire l'envoi d'e-mails à des comptes extérieurs via le serveur SMTP.
   - Le champ **Command Log Size** (Taille du journal des commandes) spécifie la taille de fichier maximale en Mo du fichier du journal des commandes.

     REMARQUE : Ce champ apparaît uniquement lorsque vous ouvrez une session pour gérer Server Administrator Web Server.
   - Le champ **Support Link** (Lien d'assistance) précise l'URL de la société qui fournit un support pour votre système géré.
   - Le champ **Délimiteur personnalisé** spécifie le caractère utilisé pour séparer les champs de données dans les fichiers créés à l'aide du bouton **Exporter**. Le caractère **;** est le délimiteur par défaut. Les autres options disponibles sont **!**, **@**, **#**, **$**, **%**, **^**, *, **~**, **?**,**|** et .
   - Le champ **Chiffrement SSL** indique une connexion sécurisée entre le serveur Web et le navigateur. Choisissez les chiffrements qui prennent en charge le serveur Web lors de la configuration. Le service de connexion ne démarre pas si une suite de chiffrement non valide est définie. Par défaut, les éléments suivants sont les valeurs de suite de chiffrement :

     `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,`

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

TLS_RSA_WITH_AES_128_CBC_SHA256,

TLS_RSA_WITH_AES_128_CBC_SHA,

TLS_RSA_WITH_AES_256_CBC_SHA256,

TLS_RSA_WITH_AES_256_CBC_SHANOTE

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

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

  REMARQUE : Si le protocole n'est pas pris en charge par les configurations par défaut, activez le protocole SSL à partir des paramètres du navigateur.
- **Algorithme de signature clé (pour le certificat auto-signé)** : vous permet de sélectionner un algorithme de signature pris en charge. Si vous sélectionnez l'algorithme **SHA 512** ou **SHA 256**, assurez-vous que votre système d'exploitation/navigateur le prend en charge. Si vous sélectionnez l'une de ces options sans la prise en charge du système d'exploitation/navigateur nécessaire, Server Administrator affiche l'erreur suivante : `impossible d'afficher la page Web`. Ce champ est destiné uniquement aux certificats auto-signés et auto-générés de Server Administrator. La liste déroulante est grisée si vous importez ou générer de nouveaux certificats dans Server Administrator.
- **Java Runtime Environment** (Environnement d'exécution Java) : vous permet de sélectionner l'une des options suivantes :
  - **Bundled JRE** (Environnement d'exécution Java groupé) : permet d'utiliser le JRE fourni avec le System Administrator.
  - **JRE système** : permet d'utiliser le JRE installé sur le système. Sélectionnez la version requise dans la liste déroulante.

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

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

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

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

Gestion du certificat X.509

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

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

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

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

Les options disponibles sont les suivantes :

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

REMARQUE : Lors de l'utilisation d'un certificat auto-signé, la plupart des navigateurs Web affichent un avertissement *non de confiance* car le certificat auto-signé n'est pas signé par une autorité de certification (AC) de confiance du système d'exploitation. Certains paramètres de navigateur sécurisés peuvent également bloquer les certificats SSL auto-signés. L'interface GUI Web de Server Administrator requiert un certificat signé par une autorité de certification pour de tels navigateurs sécurisés.

- **Certificate Maintenance** (Maintenance de certificats) : vous permet de générer une requête de signature de certificat (RSC) comprenant des informations sur l'hôte requis par l'autorité de certification pour automatiser la création d'un certificat Web SSL de confiance. Vous pouvez récupérer le fichier RSC nécessaire depuis les instructions qui figurent sur la page (RSC) ou en copiant le texte complet dans la boîte de texte qui se trouvent sur la page de RSC et en le collant dans le formulaire de l'autorité de certification. Le texte doit être au format codé Base64.

  REMARQUE : Vous pouvez également afficher les informations du certificat et exporter le certificat en cours d'utilisation au format Base64, qui peut être importé par d'autres services Web.
- **Importer une chaîne de certificat** : cette option vous permet d'importer la chaîne de certificat (au format PKCS # 7) signé par une AC de confiance. Le certificat peut être dans un format encodé Base64 ou DER.
- **Importer un magasin de clés PKCS12** : cette fonctionnalité vous permet d'importer un magasin de clés PKCS#12 qui remplace la clé privée et le certificat utilisés dans le serveur Web de Serveur Administrator. PKCS#12 est le magasin de clés public qui contient une clé privée et le certificat d'un serveur Web. Server Administrator utilise le format Java KeyStore (JKS) pour stocker les certificats SSL et sa clé privée. L'importation d'un magasin de clés PKCS#12 sur Server Administrator entraîne la suppression des entrées du magasin de clés et importe une clé privée et des entrées de certificat sur le JKS de Server Administrator.

  REMARQUE : Un message d'erreur s'affiche si vous sélectionnez un fichier PKCS non valide ou saisissez un mot de passe incorrect.

Certificats de serveur SSL

Le serveur Web Server Administrator est configuré pour utiliser le protocole de sécurité SSL (standard dans l'industrie) pour transférer des données cryptées dans un réseau. SSL repose sur une technologie de cryptage asymétrique et est largement utilisé dans les communications authentifiées et cryptées entre les clients et les serveurs pour prévenir l'écoute illicites sur les réseaux.

Un système SSL peut effectuer les tâches suivantes :

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

Le processus de cryptage fournit un haut niveau de protection des données. Server Administrator utilise la forme la plus fiable de cryptage généralement disponible pour les navigateurs Internet en Amérique du Nord.

Le serveur Web Server Administrator possède un certificat numérique SSL unique auto-signé Dell par défaut. Vous pouvez remplacer ce certificat SSL par défaut par un certificat signé par une autorité de certification (CA) connue. Une autorité de certification est une entité commerciale reconnue dans l'industrie de la technologie informatique pour répondre de manière fiable aux normes exigeantes en matière de filtrage, d'identification et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples de CA. Pour initialiser le processus d'obtention d'un certificat signé par une autorité de certification, utilisez l'interface Web Server Administrator pour générer une Requête de signature de certificat (RSC), accompagnée des informations sur votre société. Soumettez ensuite la RSC générée à une CA telle que VeriSign ou Thawte. La CA peut être une CA racine ou intermédiaire. Après réception du certificat SSL signé par une CA, chargez-le sur Server Administrator.

Le certificat SSL de chaque Server Administrator que la station de gestion doit approuver doit être placé dans le magasin de certificats de la station de gestion. Une fois le certificat SSL installé sur les stations de gestion, les navigateurs pris en charge peuvent accéder à Server Administrator sans renvoyer d'avertissements de certificat.

Onglets d'actions de Server Administrator Web Server

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

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

Mise à niveau du serveur Web

PRÉCAUTION : Le rétablissement des paramètres définis à l'usine est impossible après une mise à jour du serveur Web. Pour effectuer un tel rétablissement, réinstallez le Server Administrator.

Vous pouvez mettre à niveau le serveur Web Apache Tomcat, lorsque cela est nécessaire, à l'aide de l'**omwsupdateutility**, sans affecter les fonctionnalités de Server Administrator. L'utilitaire permet une mise à niveau vers une version secondaire de serveur Web, mais ne prend pas en charge une mise à niveau vers une version majeure. Par exemple, la mise à niveau à partir de la version A.*x* vers A.*y* est prise en charge, mais pas A.*x* vers B.*x* ou B.*y*. Par ailleurs, à l'aide de l'utilitaire, vous pouvez remplacer la version du serveur Web par une version antérieure, à condition qu'il s'agisse d'une version secondaire. L'utilitaire est enregistré à l'emplacement suivant par défaut lors de l'installation du serveur Web :

- Sur les systèmes exécutant un système d'exploitation Windows : `C :\Program Files\Dell\SysMgt\omsa\wsupdate`
- Sur les systèmes exécutant un système d'exploitation Linux : `/opt/dell/srvadmin/lib64/openmanage/wsupdate`

Vous pouvez télécharger la version requise de packages de serveur Web Tomcat et exécuter l'utilitaire à partir d'une invite de commande. Téléchargez le package de distribution de base du serveur Web Tomcat depuis `tomcat.apache.org`. Le package de distribution doit être un fichier .zip ou .tar.gz ; les packages enveloppes (wrapper) du programme d'installation Windows ne sont pas pris en charge.

Pour mettre à jour un serveur Web, recherchez le dossier **wsupdate**, puis exécutez la commande suivante :

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

Le chemin d'accès au dossier **SysMgt** par défaut est `C :\Program Files\Dell\SysMgt` et le chemin d'accès du dossier **srvadmin** est `/opt/dell/srvadmin`.

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

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

L'interface de ligne de commande (CLI) permet à un utilisateur qui a une tâche bien définie à l'esprit de récupérer rapidement les informations relatives au système. À l'aide des commandes de la CLI, par exemple, les administrateurs peuvent écrire des programmes ou des scripts par lots à des moments spécifiques. Lors de l'exécution de ces programmes, ils peuvent enregistrer des rapports sur des composants qui les intéressent, tels que les RPM des ventilateurs. Avec des scripts supplémentaires, l'utilisateur peut utiliser la CLI pour capturer des données pendant les périodes de forte utilisation du système afin de les comparer aux mêmes mesures à des moments de faible utilisation du système. Les résultats de la commande peuvent être acheminés vers un fichier en vue d'une analyse ultérieure. Grâce aux rapports, les administrateurs peuvent obtenir des informations qui leur serviront à ajuster les modes d'utilisation afin de justifier l'achat de nouvelles ressources système ou de se concentrer 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 Server Administrator* à l'adresse `dell.com/openmanagemanuals`.

4

Services Server Administrator

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

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

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

REMARQUE : Pour en savoir plus sur la configuration SNMP, voir Configuration de l'agent SNMP pour les systèmes exécutant des systèmes d'exploitation Windows pris en charge.

Sujets :

Gestion de votre système

Par défaut, la page d'accueil de Server Administrator est définie sur l'objet Système de la vue de l'arborescence système. Par défaut, pour l'objet **Système**, les composants **Intégrité** s'affichent sous l'onglet **Propriétés**.

Par défaut, la page d'accueil **Préférences** ouvre **Configuration des nœuds**.

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

REMARQUE : Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. Cliquez sur **Aide**() pour ouvrir une fenêtre d'aide indépendante contenant des informations détaillées sur la fenêtre spécifique que vous visualisez. L'aide en ligne est conçue pour vous guider tout au long des actions spécifiques nécessaires à l'exécution de tous les aspects des services Server Administrator. L'aide en ligne est disponible pour toutes les fenêtres que vous pouvez afficher, en fonction des groupes de logiciels et de matériel détectés par Server Administrator sur le système et du niveau de privilèges de l'utilisateur.

REMARQUE : Vous devez disposer de droits d'utilisateur privilégié ou de privilèges administrateur pour afficher la plupart des objets de l'arborescence système, des composants système, des onglets d'action et des fonctionnalités des zones de données configurables. En outre, seuls les utilisateurs connectés avec des privilèges d'administrateur ont accès aux fonctionnalités système critiques, telles que la fonctionnalité d'arrêt disponible dans l'onglet **Arrêt**.

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

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

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

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

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

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

Les fonctionnalités non prises en charge sur ESXi 5.X sont les suivantes :

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

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

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

Enceinte modulaire

REMARQUE : Dans le cadre de Server Administrator, le boîtier modulaire fait référence à un système qui peut contenir un ou plusieurs systèmes modulaires qui s'affichent en tant que module de serveur distinct dans l'arborescence du système. À l'instar d'un module de serveur autonome, un boîtier modulaire contient tous les composants essentiels d'un système. À la seule différence qu'une enceinte modulaire comporte des emplacements pour au moins deux modules de serveur dans un plus grand conteneur et que 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**.

- **Onglet : Propriétés**
- **Sous-onglet : 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 de **connexion** de (Chassis Management Controller) à partir de la page d'accueil de Server Administrator :

1. Cliquez sur l'objet **Boîtier modulaire**
2. Cliquez sur l'onglet **Informations CMC**, puis cliquez sur **Lancer l'interface Web CMC**. La fenêtre de **connexion** de CMC s'affiche.

Vous pouvez surveiller et gérer votre boîtier modulaire après vous être connecté au CMC.

Propriétés du système/Module de serveur

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

Licences

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

Sous le sous-onglet Licensing, vous pouvez :

- Définir les préférences pour utiliser l'iDRAC (Dell Remote Access Controller) pour importer, exporter, supprimer ou remplacer la licence numérique du matériel.
- Afficher les détails du périphérique utilisé. Les détails incluent la condition de la licence, la description de la licence, l'ID de droit et la date d'expiration de la licence.

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

  REMARQUE : Cette fonction est disponible uniquement si la version minimale requise de l'iDRAC est installée.

Propriétés

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

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

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

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

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

  REMARQUE : La fonctionnalité de la fonction du registre d'horloge de la surveillance ne peut être garantie lorsqu'un événement de mémoire non corrigible survient dans la mémoire DRAM Bank_1 du système. Si un événement de mémoire non corrigible survient dans cet emplacement, le code BIOS résidant dans cet espace peut devenir corrompu. Étant donné que la fonction d'horloge appelle le BIOS pour effectuer un comportement d'arrêt ou de redémarrage, elle peut ne pas fonctionner correctement. Si cela se produit, vous devez redémarrer le système manuellement. Le registre d'horloge de la surveillance peut être défini 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 a lieu uniquement lorsque la température signalée par le capteur dépasse le seuil de température. Un arrêt thermique ne se produit pas lorsque la température signalée par le capteur est inférieure au seuil de température.
- Arrêter le service de connexion DSM SA (serveur Web).

  REMARQUE : Server Administrator est toujours disponible via l'interface de ligne de commande (CLI) si DSM SA Connection Service est arrêté. Les fonctions de la CLI ne nécessitent pas que DSM SA Connection Service soit en cours d'exécution.

Journaux

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

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

- Afficher le journal ESM (Embedded System Management - Journal de gestion du système intégré) ou le journal SEL (System Event Log - Journal d'événements du système) pour voir une liste de tous les événements associés aux composants du matériel de votre système. L'icône du voyant d'état en regard du nom du journal passe d'une condition normale () à une condition non critique () lorsque le fichier journal atteint 80 pour cent de sa capacité. Sur les systèmes Dell PowerEdge 11G, l'icône du voyant d'état en regard du nom du journal passe à une condition critique () lorsque le fichier journal atteint une capacité de 100 pourcent.

  REMARQUE : L'activation de la fonction **Sauvegarde automatique et suppression des entrées du journal ESM** vous permet de créer une sauvegarde automatique des journaux ESM. Cette fonction n'est disponible que sur les serveurs PowerEdge 10e et 11e générations. L'iDRAC offre des fonctionnalités de sauvegarde automatique et de suppression du journal SEL sur les systèmes Dell PowerEdge de 12e génération et versions ultérieures. Seule la dernière version du fichier de sauvegarde XML est disponible dans les emplacements susmentionnés.
- Voir le journal des alertes pour afficher une liste de tous les événements générés par Server Administrator Instrumentation Service quand la condition des capteurs et des autres paramètres surveillés change.

  REMARQUE : Pour en savoir plus sur chaque ID d'événement d'alerte et sur la description de chacun, son niveau de gravité et sa cause, voir le *Server Administrator Messages Reference Guide* (Guide de référence des messages de Server Administrator) à l'adresse `dell.com/openmanagemanuals`.
- Voir le journal des commandes pour afficher une liste de chaque commande exécutée à partir de la page d'accueil de **Server Administrator** ou à partir de son interface de ligne de commande.

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

Gestion des alertes

Sous-onglets : 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 les paramètres actuels du filtres d'événements de plate-forme et définir les actions d'alerte à effectuer si le capteur d'un composant système donne une valeur d'avertissement ou de panne. Vous pouvez aussi utiliser l'option **Configurer la destination** pour sélectionner la destination (adresse IPV4 ou IPV6) d'une alerte relative à un événement de plate-forme.

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

- Afficher les seuils d'alerte d'interruptions SNMP actuels et définir les niveaux de seuil d'alerte pour les composants système d'instrumentation. Les traps sélectionnés sont déclenchés si le système génère un événement correspondant au niveau de gravité sélectionné.
  - Le **Test d'interruption SNMP** envoie l'interruption vers la destination sélectionnée à partir de la liste des destinations configurées affichée. Le composant SNMP de Server Administrator doit être installé pour l'envoi de l'interruption de test. L'administrateur doit configurer les adresses IP/le FQDN dans le service SNMP du système d'exploitation ou le fichier de configuration pour obtenir la liste des destinations d'interruptions.

    REMARQUE : Cette fonction n'est pas prise en charge sur VMware ESXi.
  - La fenêtre **Activer les interruptions SNMP** permet de configurer les paramètres d'un composant en utilisant une case à cocher et un bouton radio. La sélection d'un bouton radio modifie l'état de la case à cocher correspondante ; la désélection du bouton radio modifie aussi l'état de la case à cocher correspondante.

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

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

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 de session** et mettre fin aux sessions des utilisateurs connectés.

Châssis de système principal/Système principal

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

Les composants disponibles sont :

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

REMARQUE : L'option **Blocs d'alimentation** n'est pas disponible sur les systèmes Dell PowerEdge 1900. Les fonctions Surveillance des blocs d'alimentation et Surveillance de l'alimentation sont disponibles uniquement sur les systèmes sur lesquels sont installés au moins deux blocs d'alimentation redondants remplaçables à chaud. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondants installés de manière permanente qui ne disposent pas de circuits de gestion de l'alimentation.

Propriétés du châssis de système principal/système principal

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

Propriétés

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

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

- Afficher l'intégrité ou la condition des composants matériels et des capteurs. Une icône System/Server Module Component Status Indicators (Voyants de condition du composant du système/serveur) se trouve en regard du nom de chaque composant répertorié.  indique qu'un composant est intègre (normal).  Indique que le composant a une condition d'avertissement (non critique) et qu'il doit être vérifié.  indique qu'un composant a une condition défaillante (critique) et qu'il nécessite une intervention immédiate.  indique que la condition d'intégrité du composant est inconnue. Les composants surveillés disponibles comprennent :
  - Batteries
  - Ventilateurs
  - Journal du matériel
  - Intrusion
  - 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 de 10e génération. Les **blocs d'alimentation** ne sont pas disponibles sur Dell PowerEdge 1900. La **Gestion de l'alimentation** est prise en charge sur certains systèmes Dell PowerEdge de 10e génération. Les fonctionnalités **Surveillance des blocs d'alimentation** et **Surveillance de l'alimentation** sont disponibles uniquement pour les systèmes possédant deux blocs d'alimentation redondants et remplaçables à chaud ou plus. Ces fonctionnalités ne sont pas disponibles pour les blocs d'alimentation non redondants installés de manière permanente qui ne disposent pas de circuits de gestion de l'alimentation.

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

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

Batteries

Cliquez sur l'objet **Batteries** pour afficher des informations sur les batteries installées dans le système. Les batteries conservent la date et l'heure de mise hors tension du système. La batterie enregistre la configuration du BIOS du système 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 : batteries

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

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

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

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

BIOS

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

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

Propriétés

Sous-onglet : Informations

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

Configuration

Sous-onglet : BIOS

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

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

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

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

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

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

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

Vous pouvez définir un mot de passe de configuration du BIOS sur la page **Sécurité système**. Si vous avez défini le mot de passe de configuration, saisissez-le pour activer et modifier les paramètres du BIOS. Sans quoi les paramètres du BIOS apparaissent en mode Lecture seule. Redémarrez le système après avoir défini le mot de passe.

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

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

Ventilateurs

Cliquez sur l'objet **Ventilateurs** pour gérer les ventilateurs de votre système. Server Administrator surveille l'état de chaque ventilateur du système en mesurant les RPM. Les capteurs de ventilateurs communiquent les RPM au Server Administrator Instrumentation Service.

Lorsque vous sélectionnez Ventilateurs dans l'arborescence des appareils, des informations s'affichent dans la zone de données dans le panneau à droite de la fenêtre 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 capteurs des ventilateurs du système et configurer les valeurs minimales et maximales des seuils d'avertissement des capteurs des ventilateurs.

  REMARQUE : Certains champs de capteurs de ventilateurs varient en fonction du type de firmware installé dans le système : BMC ou ESM. Certaines valeurs de seuil ne peuvent pas être modifiées sur les systèmes dotés d'un 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.
- Définissez les niveaux des seuils d'alerte des ventilateurs.

Micrologiciel

Cliquez sur l'objet **Firmware** pour gérer le firmware de votre système. Le firmware comprend des programmes ou des données qui ont été écrites sur la ROM. Le firmware peut démarrer et fonctionner sur un appareil. Chaque contrôleur contient des firmwares qui garantissent la fonctionnalité du contrôleur. La fenêtre d'action de l'objet **Firmware** peut comporter 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 firmware du système.

Performances matérielles

Cliquez sur l'objet **Performances matérielles** pour afficher l'état et la cause de la dégradation des performances du système. La fenêtre d'action de l'objet **Performances matérielles** peut disposer de l'onglet suivant, en fonction des privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

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

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

Tableau 10. Valeurs possibles pour la condition et la cause d'un capteur

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

Intrusion

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

Propriétés

Sous-onglet : Intrusion

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

Gestion des alertes

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

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

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

Mémoire

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

Propriétés

Sous-onglet : Memory (Mémoire)

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

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

Gestion des alertes

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

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

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

Réseau

Cliquez sur l'objet **Réseau** pour gérer les cartes NIC du système. Server Administrator surveille l'état de chaque carte NIC présente sur votre système afin de garantir une connexion à distance continue. Server Administrator signale les fonctionnalités FCoE et iSoE des cartes NIC. En outre, les détails de l'association de la carte NIC sont communiqués s'ils sont déjà configurés sur le système. Deux cartes NIC physiques ou plus peuvent être regroupées en une seule carte NIC logique, à laquelle un administrateur peut attribuer une adresse IP. L'association peut être configurée à l'aide d'outils de fournisseurs de cartes NIC. Par exemple, Broadcom — BACS. Si l'une des cartes NIC physiques tombe en panne, l'adresse IP reste accessible car elle est liée à la carte NIC logique plutôt qu'à une seule carte NIC physique. Si l'interface de groupe est configurée, les propriétés détaillées du groupe s'affichent. La relation entre les cartes NIC physiques et l'interface de groupe, et vice versa, est également communiquée, si ces cartes NIC physiques font partie de l'interface de groupe.

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

REMARQUE : L'ordre dans lequel les périphériques sont détectés ne correspondra pas nécessairement à celui des ports physiques du périphérique. Cliquez sur le lien hypertexte sous Nom de l'interface pour afficher les informations sur la carte réseau.

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

REMARQUE : Server Administrator prend uniquement en charge l'inventaire des interfaces réseau physiques et leurs propriétés. Server Administrator ne prend pas en charge l'inventaire des interfaces logiques comme VLAN et Bonded.

La fenêtre d'action de l'objet **Réseau** peut comporter 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.

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

Ports

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

REMARQUE : Les ports USB CMC connectés à des serveurs lames ne sont pas énumérés par Server Administrator.

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

Sous-onglet : Informations

Propriétés

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

Gestion de l’alimentation

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

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 marge instantanée et la réserve maximale du système. Les valeurs s’affichent en watts et en BTU/h (unité thermique britannique). Les seuils d’alimentation peuvent être définis en watts et en 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 de voir les attributs Inventaire de l’alimentation tels que Alimentation inactive du système et Alimentation maximum potentielle du système en Watt et BTU/h. Vous pouvez également utiliser l’option Bilan énergétique pour activer option Alimentation maximale et définir l’alimentation maximale pour 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 du système. Server Administrator surveille l’état des blocs d’alimentation, notamment la redondance, de sorte que chaque bloc d’alimentation présent sur le système fonctionne correctement.

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

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

Propriétés

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 micrologicielle du bloc d'alimentation et la puissance de sortie maximale.
- 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 Puissance d’entrée nominale s’affiche uniquement sur les systèmes PMBus à partir de la version 11G.

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 d'alerte d'interruption SNMP actuels et définir les niveaux de seuil d'alerte pour la puissance système (Watts). Les traps sélectionnés sont déclenchés si le système génère un événement correspondant au niveau de gravité sélectionné.

REMARQUE : L'interruption Puissance système maximale génère des événements uniquement pour indiquer la gravité.

Processeurs

Cliquez sur l'objet **Processeurs** pour gérer les microprocesseurs du système. Un processeur est la puce de calcul principal d'un système, qui contrôle l'interprétation et l'exécution des fonctions arithmétiques et logiques. La fenêtre d'action de l'objet Processeurs peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Sous-onglet : Informations

Propriétés

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

Gestion des alertes

Sous-onglets : 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.

En sélectionnant l'onglet Accès distant, vous pouvez gérer les fonctionnalités du BMC/iDRAC, telles que les informations générales relatives au BMC/iDRAC. Vous pouvez également gérer la configuration du BMC/iDRAC sur un réseau local (LAN), un port série pour le BMC/iDRAC, les paramètres du mode terminal pour le port série, le BMC/iDRAC sur une connexion série sur LAN et les utilisateurs BMC/iDRAC.

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

Utilisez le DRAC pour accéder aux fonctionnalités de gestion du système distant de votre système. Le DRAC Server Administrator fournit un accès à distance à des systèmes inutilisables, une notification d'alerte lorsqu'un système est en panne 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.

Sous-onglet : Informations

Propriétés

Sous l'onglet **Propriétés**, vous pouvez afficher les informations générales sur l'appareil 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.

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

Configuration

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

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

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

Sous l'onglet **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 utilisateur de l'accès à distance. Vous pouvez ajouter, configurer et afficher des informations relatives aux utilisateurs du contrôleur d'accès à distance.

Média flash amovible

Cliquez sur l'objet **Support Flash amovible** pour afficher l'état d'intégrité et de redondance des modules SD internes et du support vFlash. La fenêtre d'action **Support Flash amovible** comporte l'onglet **Propriétés** .

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, vous pouvez consulter des informations sur le support Flash amovible et les modules SD internes. Parmi elles figurent des détails sur le nom du connecteur, son état et la taille de stockage.

Gestion des alertes

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

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

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

La gestion des alertes est courante pour les modules SD internes et vFlash. La configuration d'actions d'alertes/SNMP/PEF pour les modules SD ou les supports vFlash entraîne automatiquement leur configuration pour les uns ou les autres.

Emplacements

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

Propriétés

Sous-onglet : Informations

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

Températures

Cliquez sur l'objet **Températures** pour gérer la température de votre système afin d'éviter tout dommage thermique des composants internes de votre système. Server Administrator surveille la température dans divers emplacements du châssis du système afin de garantir que les températures à l'intérieur du châssis ne deviennent pas trop élevées.

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

Sous-onglet : Capteurs de température

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

REMARQUE : Certains champs de capteurs de température varient en fonction du type de firmware installé dans le système : BMC ou ESM. Certaines valeurs de seuil ne peuvent pas être modifiées sur les systèmes dotés d'un contrôleur BMC. Lorsque vous

définissez des seuils de capteur, Server Administrator arrondit parfois les valeurs minimale ou maximale que vous entrez à la valeur définissable la plus proche.

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 température renvoie une valeur d'avertissement ou de panne.
- Afficher les seuils d'alertes d'interruptions SNMP actuels et définir les niveaux des seuils d'alerte des capteurs de température. Les traps sélectionnés sont déclenchés si le système génère un événement correspondant au niveau de gravité sélectionné.

REMARQUE : Pour un châssis externe, vous pouvez définir uniquement des entiers comme valeurs de seuil minimal et maximal de capteur de températures. Si vous tentez de définir une valeur de seuil minimal ou maximal de capteur de températures avec un nombre décimal, seul le nombre entier avant la virgule est enregistré en tant que paramètre de seuil.

Tensions

Cliquez sur l'objet **Tensions** pour gérer les niveaux de tension de votre système. Server Administrator surveille les tensions entre les composants critiques dans divers emplacements du châssis sur 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 : Capteurs de tension

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

REMARQUE : Certains champs de capteurs de tension varient en fonction du type de firmware installé dans le système, comme BMC ou ESM. Certaines valeurs de seuil ne peuvent pas être modifiées sur les systèmes dotés d'un contrôleur BMC.

Gestion des alertes

Sous-onglets : Actions d'alerte | Interruptions SNMP

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 capteur de tension du système renvoie une valeur d'avertissement ou de panne.
- Afficher les seuils d'alertes d'interruptions SNMP actuels et définir les niveaux des seuils d'alerte des capteurs de tension. Les traps sélectionnés sont déclenchés si le système génère un événement correspondant au niveau de gravité sélectionné.

Logiciel

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

Sous-onglet : synthèse

Propriétés

Sous l'onglet **Propriétés**, vous pouvez consulter une synthèse du système d'exploitation et du logiciel de gestion du système surveillé.

Système d'exploitation

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

Propriétés

Sous-onglet : Informations

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

Stockage

Server Administrator inclut Storage Management Service :

Storage Management Storage propose des fonctionnalités de configuration pour les appareils de stockage. Dans la plupart des cas, Storage Management Service est installé avec la **Configuration typique**. Storage Management Service est disponible sur les systèmes d'exploitation Microsoft Windows, Red Hat Enterprise Linux et SUSE Linux Enterprise Server.

Lors de l'installation de Storage Management Service, cliquez sur l'objet **Stockage** pour afficher l'état et les paramètres de plusieurs appareils de stockage de baie, disques système, etc.

Dans le cas de Storage Management Service, la fenêtre d'action de l'objet Stockage contient 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 l'état des composants de stockage et des capteurs connectés, tels que les sous-systèmes de baie et les disques du système d'exploitation.

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

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

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

- Paramètres généraux
- Server Administrator

Paramètres généraux

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

Sous-onglet : Properties (Propriétés)

Utilisateur

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**.

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

Sous l'onglet Web Server, vous pouvez :

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

Server Administrator

Cliquez sur l'objet **Server Administrator** pour autoriser ou interdire l'accès aux utilisateurs dotés de privilèges d'utilisateur ou d'utilisateur privilégié. La fenêtre d'action de l'objet **Server Administrator** peut comporter l'onglet suivant, selon les privilèges du groupe de l'utilisateur : **Préférences**.

Sous-onglets : Configuration de l’accès

Préférences

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

5

Utilisation de Remote Access Controller

Le contrôleur BMC (Baseboard Management Controller - Contrôleur de gestion de la carte de base)/iDRAC (Integrated Dell Remote Access Controller - Contrôleur d'accès à distance Dell intégré) surveille le système et détecte les événements critiques en communiquant avec différents capteurs de la carte système, et envoie des alertes et des événements de journal lorsque certains paramètres dépassent leurs seuils prédéfinis. Le contrôleur BMC/iDRAC prend en charge la spécification IPMI (Intelligent Platform Management Interface) standard pour vous permettre de configurer, surveiller et restaurer les systèmes à distance.

REMARQUE : Le contrôleur iDRAC (Integrated Dell Remote Access Controller) est pris en charge par les systèmes PowerEdge de 10e génération et ultérieurs.

Le DRAC est une solution matérielle et logicielle de gestion de systèmes conçue pour fournir des fonctionnalités de gestion à distance, de récupération d'un système suite à une panne et de contrôle de l'alimentation.

En communiquant avec le contrôleur BMC (Baseboard Management Controller - Contrôleur de gestion de la carte de base)/iDRAC (Integrated Dell Remote Access Controller - Contrôleur d'accès à distance Dell intégré) du système, le DRAC peut être configuré pour vous envoyer par e-mail des alertes sur les avertissements ou erreurs liés à la tension, à la température et à la vitesse de ventilateur. Le DRAC journalise également les données d'événement et l'écran de défaillance le plus récent (uniquement disponible sur les systèmes qui exécutent un système d'exploitation Microsoft Windows) pour vous aider à diagnostiquer la cause probable d'une défaillance du système.

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

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

Lorsque vous utilisez le Remote Access Controller, vous pouvez cliquer sur **Aide** pour obtenir des informations détaillées sur la fenêtre affichée. L'aide du Remote Access Controller est disponible pour toutes les fenêtres auxquelles l'utilisateur a accès, en fonction des privilèges dont il dispose et des groupes matériels et logiciels spécifiques détectés par Server Administrator sur le système géré.

REMARQUE : Pour en savoir plus sur le BMC, voir le document *Guide de l'utilisateur du contrôleur de gestion de la carte de base de Dell EMC* à l'adresse `dell.com/systemsecuritymanuals`.

REMARQUE : Pour des informations détaillées sur la configuration et l'utilisation de l'iDRAC, voir le *Guide de l'utilisateur de l'Integrated Dell Remote Access Controller* à l'adresse `dell.com/systemsecuritymanuals`.

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

Tableau 11. Noms des champs de l'interface utilisateur graphique et du système applicable

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

Pour en savoir plus sur la prise en charge de périphériques d'accès à distance par le système, voir le document *Matrice de prise en charge logicielle des systèmes Dell EMC* à l'adresse **dell.com/openmanagemanuals**.

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

Vous pouvez réaliser les tâches suivantes :

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

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

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

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

Sujets :

Affichage des informations de base

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

REMARQUE : Pour rétablir les paramètres BMC, vous devez être connecté avec des privilèges d'administrateur.

Cliquez sur l'objet **Enceinte modulaire** > **Système/Module de serveur** > **Châssis du système principal/Système principal** > **Accès distant**

La page **Accès distant** affiche les informations de base suivantes concernant le BMC du système :

Périphérique d'accès à distance

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

Adresse IPv4

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

Adresse IPv6

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

- Source d'adresse DNS
- Serveur DNS préféré
- Serveur DNS auxiliaire

REMARQUE : Vous ne pouvez voir les détails des adresses IPv4 et IPv6 que si vous activez les propriétés IPv4 et IPv6 sous **Configuration supplémentaire** dans l'onglet **Accès distant**.

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 de système principal/Système principal** > **Accès distant**.
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **LAN**.

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

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

4. Spécifiez les détails de configuration du NIC suivants :
   - Activer le NIC (Sélectionnez cette option pour le regroupement des cartes réseau.)

   REMARQUE : Votre DRAC contient une carte NIC Ethernet 10BASE-T/100BASE-T intégrée et prend en charge les TCP/IP. La carte NIC possède une adresse par défaut (192.168.20.1) et une passerelle par défaut de (192.168.20.1).

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

   REMARQUE : La modification de l'adresse IP du DRAC provoque la réinitialisation de ce dernier. Si le SNMP interroge le DRAC avant sa réinitialisation, un avertissement de température est enregistré dans le journal, car la température n'est correctement communiquée qu'une fois le DRAC initialisé.

   - Sélection de NIC

   REMARQUE : L'option Sélection de NIC ne peut pas être configurée sur les systèmes modulaires.

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

   - Options de réseau principal et de basculement

   Pour les systèmes 12G, les options du réseau principal pour la carte `NIC` Remote Management (iDRAC7) sont les suivantes : `LOM1`, `LOM2`, `LOM3`, `LOM4` et `Dédié`. Les options du réseau de basculement sont les suivantes : `LOM1`, `LOM2`, `LOM3`, `LOM4`, `All LOM` et `Aucun`.

   REMARQUE : L'option `Dedicated` est disponible lorsqu'il existe une licence iDRAC7 Enterprise valide. Le nombre de LOM varie selon la configuration du système ou du matériel.

   - Activer IPMI sur le LAN
   - Source d'adresse IP
   - Adresse IP
   - Masque de sous-réseau
   - Adresse de passerelle
   - Limite du niveau de privilège du canal
   - Nouvelle clé de cryptage
5. Spécifiez les détails suivants de la configuration du VLAN en option :

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

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

6. Configurez les propriétés IPv4 suivantes :
   - Source d'adresse IP
   - Adresse IP
   - Masque de sous-réseau
   - Adresse de passerelle
7. Configurez les propriétés IPv6 suivantes :
   - Source d'adresse IP
   - Adresse IP
   - Longueur du préfixe
   - Passerelle par défaut
   - Source d'adresse DNS
   - Serveur DNS préféré
   - Serveur DNS auxiliaire

   REMARQUE : Vous êtes en mesure de configurer les détails relatifs aux adresses IPv4 et IPv6 uniquement si vous activez les propriétés IPv4 et IPv6 sous **Configuration supplémentaire**.
8. Cliquez sur **Appliquer les modifications**.

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

Pour configurer le BMC pour les communications sur une connexion de port série :

1. Cliquez sur l'objet **Boîtier modulaire** > **Système/Module de serveur** > **Châssis du système principal/Système principal** > **Accès distant**.
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Port série**.

   La fenêtre **Configuration du port série** s'affiche.
4. Configurez les détails suivants :
   - Paramètre du mode de connexion
   - Débit en bauds
   - Contrôle du débit
   - Limite du niveau de privilège du canal
5. Cliquez sur **Appliquer les 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 Intelligent Platform Interface Management (IMPI) sur le port série avec des caractères ASCII imprimables. Le mode terminal prend également en charge un nombre limité de commandes texte pour prendre en charge les environnements hérités basés sur texte. Cet environnement est conçu de manière à pouvoir utiliser un simple terminal ou émulateur de terminal.
7. Spécifiez les personnalisations suivantes pour améliorer 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 **Revenir 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 **Boîtier modulaire** > **Système/Module de serveur** > **Châssis de système principal/Système principal** > **Accès distant**.
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 le LAN
   - Débit en bauds
   - Minimum de privilèges 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 de système principal/Système principal→ Accès distant**.
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Additional Configuration**.
4. Configurez les propriétés Ipv4 et IPv6 en les définissant sur **Activé** ou **Désactivé**.
5. Cliquez sur **Appliquer les modifications**.

   REMARQUE : Pour plus d'informations sur la gestion de licences, voir le *Guide de l'utilisateur de Dell License Manager* disponible sur le site `dell.com/openmanagemanuals`.

Configuration des utilisateurs du périphérique d'accès à distance

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

1. Cliquez sur l'objet **Enceinte modulaire** > **Système /Module de serveur** > **Châssis de système principal/Système principal** > **Accès distant**.
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.
   - Saisissez le nom de l'utilisateur dans le champ **Nom d'utilisateur**.
   - Cochez la case **Modifier le mot de passe**.
   - Saisissez un nouveau mot de passe dans le champ **Nouveau mot de passe**.
   - Saisissez 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.
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 : Vous pouvez configurer six entrées utilisateur supplémentaires lors de l'installation du DRAC. Vous obtiendrez alors un total de 16 utilisateurs. Les mêmes règles de nom d'utilisateur et de mot de passe s'appliquent aux utilisateurs de BMC/iDRAC et RAC. Lors de l'installation du DRAC/iDRAC6, l'ensemble des 16 entrées utilisateur sont attribuées au DRAC.

Définition des alertes de filtre d'événements sur plateforme

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

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

   La fenêtre **Platform Events** vous permet de prendre des actions individuelles en réponse à des événements spécifiques de la plateforme. Vous pouvez sélectionner les événements pour lesquels vous souhaitez prendre des actions d'arrêt et générer des alertes pour les actions sélectionnées. Vous pouvez également envoyer des alertes à des destinations d'adresses IP spécifiques de votre choix.

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

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

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

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

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

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

5. Sélectionnez l'une des actions suivantes :
   - **Aucun**
   - **Redémarrer le système**

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

   - **Arrêter le système**

Coupe l'alimentation du système.

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

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

- **Réduction de puissance.**

  Accélère l'UC.

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

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

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

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

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

Définition des destinations des alertes d'événements de plateforme

Vous pouvez aussi utiliser la fenêtre Filtres d'événements de plateforme pour sélectionner la destination d'une alerte relative à un événement de plate-forme. Selon le nombre de destinations affichées, vous pouvez définir une adresse IP distincte pour chaque adresse de destination. Une alerte d'événement de plate-forme est envoyée à chaque adresse IP de destination que vous définissez.

1. Cliquez sur **Configurer les destinations** dans la fenêtre Platform Event Filters.
2. Cliquez sur le nombre de destinations à configurer.

   REMARQUE : Le nombre de destinations que vous pouvez configurer sur un système varie.

3. Cochez la case **Activer la destination**.
4. Cliquez sur le champ **Numéro de destination** pour saisir une adresse IP individuelle pour la destination concernée. Il s'agit de l'adresse IP de destination de l'alerte relative à un événement de plate-forme.

   REMARQUE : Sur les systèmes 12G dotés de versions spécifiques iDRAC7, vous pouvez définir la destination des événements de plateforme en tant que IPv4, IPv6 ou FQDN.

5. Entrez une valeur dans le champ **Chaîne de communauté** devant faire office de mot de passe pour authentifier les messages envoyés entre la station de gestion et un système géré. La chaîne de communauté (appelée également nom de communauté) est envoyée dans chaque paquet entre la station de gestion et le système géré.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **Retour à la page Événements sur plateforme** pour revenir à la fenêtre **Platform Event Filters**.

6

Journaux de Server Administrator

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

Pour en savoir plus sur l'affichage des journaux et sur la création de rapports depuis la ligne de commande, voir le *Guide d'utilisateur de l'interface de ligne de commande de Server Administrator* à l'adresse **dell.com/openmanagemanuals**.

Lorsque vous consultez les journaux Server Administrator, vous pouvez cliquer sur **Aide** ()pour obtenir des informations détaillées sur la fenêtre affichée. L'aide du journal Server Administrator est disponible pour toutes les fenêtres auxquelles l'utilisateur a accès, en fonction des privilèges dont il dispose et des groupes matériels et logiciels spécifiques détectés par Server Administrator sur le système géré.

Sujets :

Fonctionnalités intégrées

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

Boutons de tâche des fenêtres des journaux

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

Tableau 12. Boutons de tâche des fenêtres des journaux

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

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

Journaux de Server Administrator

Server Administrator fournit les journaux suivants :

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

Journal du matériel

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

Tableau 13. Voyant d'état de journal du matériel

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

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

Les informations affichées dans les journaux ESM et SEL comprennent :

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

Maintenance du journal du matériel

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

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

Journal des alertes

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

REMARQUE : La taille du fichier journal des alertes est limitée. Pour capturer un maximum de journaux des alertes, activez tous les filtres de journal du système d'exploitation.

Utilisez le journal des alertes pour surveiller les divers événements système. Server Administrator génère des événements en réponse aux modifications de l'état des capteurs et autres paramètres surveillés. Chaque événement de modification d'état enregistré dans le journal des alertes comprend un identifiant unique (ID d'événement) pour une catégorie source d'événement spécifique et un message d'événement décrivant l'événement. Le message et l'ID d'événement décrivent de manière unique la gravité et la cause de l'événement et fournissent d'autres informations pertinentes, telles que l'emplacement de l'événement et 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 diagnostic et de dépannage ultérieur. Par conséquent, il vous est recommandé d'enregistrer les fichiers journaux.

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

Pour des informations détaillées sur les messages d'alertes, voir le *Guide de référence des messages de Server Administrator* à l'adresse **dell.com/openmanagemanuals**.

Journal des commandes

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

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

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

Les informations affichées dans le journal des commandes comprennent :

- la date et l'heure auxquelles la commande a été initiée ;
- l'utilisateur actuellement connecté à la page d'accueil de Server Administrator ou à la CLI ;
- la description de la commande et de ses valeurs connexes.

REMARQUE : L'historique du journal peut être utile à des fins de diagnostic et de dépannage ultérieur. Par conséquent, il vous est recommandé d'enregistrer les fichiers journaux.

7

Définition d'actions d'alerte

Sujets :

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

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

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

Lorsque vous définissez des actions d'alerte pour un événement, vous pouvez spécifier l'action **Exécuter une application**. Les applications que Server Administrator peut exécuter sont limitées. Pour garantir une bonne exécution :

- Ne spécifiez pas d'applications basées sur le système X Window, car Server Administrator ne peut pas 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 les commandes **stdout** et **stderr** vers un fichier lorsque vous spécifiez l'application pour pouvoir voir les éventuels messages d'erreur ou de sortie.
- Si vous voulez exécuter plusieurs applications (ou commandes) pour une alerte, créez un script à cet effet et insérez le chemin d'accès complet du script dans la zone **Chemin d'accès absolu à l'application**.

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

La commande de l'exemple 1 exécute la commande ps de l'application et redirige la commande stdout vers le fichier **/tmp/psout.txt** et la commande **stderr** vers le même fichier que la commande **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 contenu dans le fichier `/tmp/alertmsg.txt` à l'utilisateur Red Hat Enterprise Linux ou SUSE Linux Enterprise Server, ainsi qu'à l'administrateur, avec l'objet **Alerte du serveur**. L'utilisateur doit créer le fichier `/tmp/alertmsg.txt` avant que l'événement ne se produise. De plus, les commandes **stdout** et **stderr** sont redirigées vers le fichier `/tmp/mailout.txt` en cas d'erreur.

Définition des actions d'alerte sous Microsoft Windows Server 2008

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

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

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

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

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

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

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

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

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

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

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

Pour autoriser l'interaction avec le bureau :

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

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

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

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

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

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

Tableau 14. Événements d'alerte PEF

Événement	Description
Échec signalé par le capteur de ventilateur	Le ventilateur fonctionne trop lentement ou il est arrêté.
Échec signalé par le capteur de tensions	La tension est trop basse pour un fonctionnement correct.
Avertissement du capteur de batterie	La batterie fonctionne en dessous du niveau recommandé de charge.
Échec signalé par le capteur de batterie	La batterie est défaillante.
Échec signalé par le capteur discret de ventilateur	La tension est trop basse pour un fonctionnement correct.
Avertissement du capteur de température	La température devient trop élevée ou trop basse.
Échec signalé par le capteur de température	La température est trop élevée ou trop basse pour un fonctionnement normal.
Détection d'une intrusion dans le châssis	Le châssis du système a été ouvert
Redondance (bloc d'alimentation ou ventilateur) dégradée	La redondance des ventilateurs et/ou des blocs d'alimentation est réduite.
Redondance (bloc d'alimentation ou ventilateur) perdue	Aucune redondance pour les ventilateurs et/ou les blocs d'alimentation du système.
Avertissement de processeur	Les performances ou la vitesse d'un processeur ne sont pas maximales.
Échec du processeur	Un processeur est défaillant.
Processeur absent	Le processeur a été retiré.
Avertissement concernant PS/VRM/D2D	Le bloc d'alimentation, le module régulateur de tension ou le convertisseur CC-CC est sur le point d'être défaillant.
Panne de PS/VRM/D2D	Le bloc d'alimentation, le module régulateur de tension ou le convertisseur CC-CC est défaillant.
Journal du matériel plein ou vide	Un journal de matériel vide ou saturé nécessite l'intervention de l'administrateur.
Récupération automatique du système	Le système est bloqué ou ne répond pas et exécute l'action définie par la récupération automatique du système.
Avertissement du capteur d'alimentation du système	La consommation d'énergie est proche du seuil de défaillance.
Échec signalé par le capteur de puissance système	La consommation électrique a dépassé la limite maximale acceptable et a généré un échec.
Média flash amovible absent	Le média flash amovible a été retiré.
Échec du média flash amovible	Le média flash amovible est sur le point d'être défaillant.
Avertissement du média flash amovible	Le média flash amovible est sur le point d'être défaillant.
Carte du module SD double interne critique	La carte du module SD double interne est défaillante.
Avertissement de la carte du module SD double interne	La carte du module SD double interne est sur le point d'être défaillante.
Redondance perdue pour la carte du module SD double interne	La carte du module SD double interne n'a pas de redondance.
Carte du module SD double interne absente	La carte du module SD double interne a été retirée.

8

Dépannage

Échec du service de connexion

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

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

  ```
  setsebool allow_execstack on
  ```

- Modifiez le contexte de sécurité du service de connexion SM SA. Exécutez la commande suivante : `chcon -t unconfined_execmem_t/opt/dell/srvadmin/sbin/dsm_om_connsvcd`

Sujets :

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 **Ignorer l'avertissement de certificat** sur la page d'ouverture de session
- Les services Server Administrator ne sont pas activés dans le système de VMware ESXi. Pour plus d'informations sur l'activation des services Server Administrator sur le système VMware ESXi, consultez le *Guide d'installation de Server Administrator*, sur `Dell.com/openmanagemanuals`.
- Le service SFCBD (small footprint CIM broker daemon) du système VMware ESXi ne s'exécute pas.
- Le service Web Server Management Service du système géré ne s'exécute pas.
- Vous saisissez 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 Autorisation WinRM (Activation à distance) n'est pas configurée sur le système géré. Pour en savoir plus sur cette fonctionnalité, consultez le document *Guide d'installation de Server Administrator* disponible à l'adresse `dell.com/openmanagemanuals`.
- Un échec d'authentification se produit lors de la connexion à un système d'exploitation VMware ESXi 5.0 qui peut être dû à l'une des raisons suivantes :
  1. Le mode `lockdown` est activé lorsque vous vous connectez au serveur ou lorsque vous êtes connecté à Server Administrator. Pour en savoir plus sur le mode `lockdown`, consultez la documentation VMware.
  2. Le mot de passe a été modifié alors que votre session Server Administrator est active.
  3. Vous ouvrez une session Server Administrator en tant qu'utilisateur ordinaire sans privilèges d'administrateur. Pour plus d'informations, reportez-vous à la documentation VMware concernant 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 procédant ensuite à une désinstallation de Server Administrator.

Pour forcer une réinstallation :

1. Vérifiez la version de Server Administrator installée précédemment.
2. Téléchargez le progiciel d'installation de cette version-là sur **support.dell.com**.
3. Localisez `SysMgmt.msi` dans le répertoire `srvadmin\windows\SystemsManagement`.
4. Saisissez la commande suivante à l'invite de commande pour forcer une réinstallation

   ```
   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 certain des éléments initialement installés, sélectionnez-toutes les fonctionnalités et lancez l'installation.

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

   REMARQUE : Une fois l'application installée, vous pouvez désinstaller Server Administrator depuis **Ajout/Suppression de programmes**.

Services Server Administrator

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

Tableau 15. Services Server Administrator

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

Tableau 15. Services Server Administrator (suite)

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Gravité
REMARQUE : Server Administrator peut envoyer des interruptions SNMP en double ou journaliser des événements en double sur la page du journal des alertes ou dans le fichier journal du système d'exploitation. La duplication des interruptions et des événements est enregistrée lorsque les services Server Administrator sont redémarrés manuellement ou lorsque le capteur de périphérique indique encore un état anormal lors du démarrage des services Server Administrator après un redémarrage du système d'exploitation. **REMARQUE :** Le collecteur d'inventaire est requis pour mettre à jour les consoles Dell à l'aide des progiciels de mise à jour Dell (DUP). **REMARQUE :** Certaines fonctionnalités du collecteur d'inventaire ne sont pas prises en charge par Server Administrator (64 bits).				
Windows : SM SA Data Manager Linux : `dsm_sa_datamgrd` (hébergé sous le service dataeng) (Ce service s'exécute sur le système géré.)	Surveille le système, fournit un accès rapide à des informations détaillées sur les pannes et les performances, et permet l'administration à distance de systèmes surveillés, y compris l'arrêt, le démarrage et la sécurité.	Les utilisateurs ne peuvent pas configurer/afficher des détails sur le niveau matériel depuis l'interface GUI/CLI si ces services ne sont pas en cours d'exécution.	Redémarrer le service	Critique
Windows : SM SA Data Manager Linux : `dsm_sa_eventmgrd` (hébergé sous le service dataeng) (Ce service s'exécute sur le système géré.)	Fournit un service de journalisation des événements en rapport au système d'exploitation et aux fichiers en vue de la gestion de systèmes. Il est également utilisé par les analyseurs de journaux d'événements.	Si ce service est arrêté, les fonctions de journalisation des événements ne fonctionnent pas correctement.	Redémarrer le service	Avertissement
Linux : `dsm_sa_snmpd` (hébergé sous le service dataeng) (Ce service s'exécute sur le système géré.)	Interface Data Engine Linux SNMP	Les demandes SNMP get/set/trap ne fonctionnent pas à partir d'une station de gestion.	Redémarrer le service	Critique
Windows : `mr2kserv` (Ce service s'exécute sur le système géré.)	Le service Storage Management fournit des informations sur la gestion du stockage et des fonctionnalités avancées pour configurer un stockage local ou distant rattaché à un système.	Les utilisateurs ne peuvent pas exécuter de fonctions de stockage pour tous les contrôleurs RAID et non RAID pris en charge.	Redémarrer le service	Critique

9

Questions fréquemment posées

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

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

1. **Pourquoi les fonctionnalités de redémarrage des hôtes ESXi 5.x échouent-elles depuis Server Administrator ?**

   Ce problème découle de la clé de licence SAL (stand alone license - licence autonome) VMware. Pour en savoir plus, consultez l'article connexe de la base de connaissances sur **kb.vmware.com/kb/kb1026060**.
2. **Quel est le niveau de permission minimum requis pour installer Server Administrator ?**

   Pour installer Server Administrator, vous devez disposer de privilèges d'administrateur. Les utilisateurs et utilisateurs privilégiés ne sont pas autorisés à installer Server Administrator.
3. **Existe-t-il un chemin de mise à niveau requis pour installer Server Administrator ?**

   Pour les systèmes exécutant Server Administrator 4.3, vous devez effectuer une mise à niveau à une version 6.*x* puis à la version 7.*x*. Pour les systèmes exécutant une version antérieure à 4.3, vous devez effectuer une mise à niveau à la version 4.3, puis à une version 6.*x* et enfin à la version 7.*x* (*x* indique la version de Server Administrator vers laquelle vous souhaitez vous mettre à niveau).
4. **Comment puis-je déterminer la dernière version de Server Administrator disponible pour mon système ?**

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

   Toutes les versions disponibles de Server Administrator sont affichées sur la page.
5. **Comment puis-je savoir quelle version de Server Administrator s'exécute sur mon système ?**

   Une fois que vous êtes connecté à Server Administrator, naviguez vers **Properties → Summary** (Propriétés → Résumé). Vous trouverez la version de Server Administrator installée sur votre système dans la colonne **Systems Management** (Gestion des systèmes).
6. **Existe-t-il d'autres ports que les utilisateurs peuvent employer à part le port 1311 ?**

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

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

   REMARQUE : Si vous modifiez le numéro de port en le remplaçant par un numéro non valide ou déjà utilisé, les autres applications ou navigateurs risquent de ne pas pouvoir accéder à Server Administrator sur le système géré. Pour obtenir la liste des ports par défaut, consultez le *Server Administrator Installation Guide* (Guide d'installation de Server Administrator) disponible à l'adresse `dell.com/openmanagemanuals`.
7. **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.
8. **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.
9. **Le protocole SNMP est-il requis pour la découverte ITA, l'inventaire et les mises à jour logicielles sur des systèmes PowerEdge ? Le protocole CIM peut-il être utilisé seul pour la découverte, l'inventaire et les mises à jour ou SNMP est-il requis ?**

   Communication ITA *avec les systèmes Linux* :

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

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

   Communication ITA avec les systèmes Windows :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    Pour 32 bits :

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

    Pour 64 bits :

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

14. **Pourquoi le système d'exploitation Red Hat Enterprise Linux 5.9 (32 bits) n'est-il pas en mesure de détecter la carte Emulex après avoir installé les pilotes Emulex ?**

    Sur les systèmes exécutant le système d'exploitation Red Hat Enterprise Linux 5.9 (32 bits), le pilote Emulex est dépendant des RPM suivants :

    - kernel-headers-2.6.18-346.el5.i386.rpm
    - glibc-headers-2.5-107.i386.rpm
    - glibc-devel-2.5-107.i386.rpm
    - gcc-4.1.2-54.el5.i386.rpm

    Si l'un des RPM est manquant, le système éprouve de la difficulté à détecter les adaptateurs réseau Emulex.

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

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

    - `esxcli system snmp set --communities public`

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