Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

Remarques et avertissements

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

PRÉCAUTION : Un AVIS vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

Mars 2009

Retour à la page du sommaire

Définition d'actions d'alerte

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

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

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

Lorsque vous définissez les actions d'alerte d'un événement, vous pouvez spécifier que l'action **diffuse un message.** Pour effectuer cette action, Server Administrator exécute la commande **wall**, qui envoie le message à toutes les personnes connectées dont l'autorisation de messagerie est définie sur **Oui.** Par défaut, ce message ne s'affichera pas si le système Server Administrator fonctionne sous un système X Window. Pour afficher le message de diffusion quand le système X Windows s'exécute, vous devez démarrer un terminal tel que **xterm** ou **gnome-terminal** avant que l'événement ne se produise.

Lorsque vous définissez les actions d'alerte d'un événement, vous pouvez spécifier que l'action **exécute une application.** Il y a des limites aux applications que Server Administrator peut exécuter. Suivez les consignes suivantes pour que l'exécution soit correcte :

- Ne spécifiez pas d'applications de système X Window car Server Administrator est incapable d'exécuter ces applications correctement.
- Ne spécifiez pas d'applications qui nécessitent des entrées de la part de l'utilisateur car Server Administrator est incapable d'exécuter ces applications correctement.
- Redirigez **stdout** et **stderr** vers un fichier lorsque vous spécifiez l'application pour pouvoir voir les résultats ou les messages d'erreur.
- Si vous voulez exécuter plusieurs applications (ou commandes) pour une alerte, créez un script à cet effet et indiquez le chemin complet du script dans la case **Chemin absolu de l'application**.

  Exemple 1 :

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

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

  Exemple 2 :

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

  La commande de l'exemple 2 exécute l'application de messagerie pour envoyer le message du fichier **/tmp/alertmsg.txt** à l'utilisateur et à l'administrateur de Red Hat Enterprise Linux ou SUSE Linux Enterprise Server, avec le sujet **Server Alert**. Le fichier **/tmp/alertmsg.txt** doit être créé par l'utilisateur avant que l'événement ne se produise. En cas d'erreur, **stdout** et **stderr** sont alors redirigés vers le fichier **/tmp/mailout.txt**.

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

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

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

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

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

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

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

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

Tous les messages relatifs aux filtres d'événements de plateforme (PEF) possibles sont énumérés au Tableau 8-1 avec une description de chaque événement.

Tableau 8-1. Événements d'alerte PEF

Événement	Description
Panne de sonde de ventilateur	Le ventilateur fonctionne trop lentement ou pas du tout.
Panne de sonde de tension	La tension est trop basse pour un fonctionnement correct.
Panne de la sonde de tension discrète	La tension est trop basse pour un fonctionnement correct.
Avertissement des sondes de température	La température approche de ses limites excessivement hautes ou basses.
Panne de sonde de température	La température est trop haute ou trop basse pour un fonctionnement correct.
Détection d'une intrusion dans le châssis	Le châssis du système a été ouvert.
Redondance (bloc d'alimentation ou ventilateur) dégradée	La redondance des ventilateurs et/ou des blocs d'alimentation a été réduite.
Redondance (bloc d'alimentation ou ventilateur) dégradée	Plus aucune redondance n'est disponible pour les ventilateurs et/ou les blocs d'alimentation du système.
Avertissement concernant un processeur	Un processeur ne fonctionne pas à ses performances ou sa vitesse maximales.
Panne de processeur	Un processeur est en panne.
Avertissement de PPS/VRM/DCtoDC	Le bloc d'alimentation, le module de régulation de la tension ou le convertisseur CC à CC va bientôt être en condition de panne.
Panne de bloc d'alimentation/VRM/D2D	Le bloc d'alimentation, le module de régulation de la tension ou le convertisseur CC à CC est en panne.
Journal du matériel plein ou vide	Un journal du matériel plein ou vide nécessite l'attention de l'administrateur.
Récupération automatique du système	Le système est bloqué ou ne répond pas, et effectue une action configurée par la récupération automatique du système.
Avertissement de sonde de puissance système	La consommation de puissance se rapproche du seuil de panne.
Panne de sonde de puissance système	La consommation de puissance a dépassé la limite acceptable la plus élevée et a provoqué une panne.

Explication des noms de services

Les noms d'exécutables et d'affichage des services suivants ont été modifiés :

Tableau 8-2. Noms de services

Rôle	Nom de service	Version précédente (antérieure à la version 5.0)	Version actuelle
Serveur Web	Nom d'affichage	Port sécurisé Serveur	Service de connexion DSM SA
	Nom d'exécutable	Omaws[32|64]	dsm_om_connsvc[32|64]
			dsm_om_connsvc
Planification ou notification	Nom d'affichage	Services communs OM	Services partagés DSM SA
	Nom d'exécutable	Omsad[32|64]	dsm_om_shrsvc[32|64]
			dsm_om_shrsvc

Retour à la page du sommaire

Retour à la page du sommaire

Dépannage

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

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 n'est pas sous tension ;
- 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 si vous ne sélectionnez pas l'**avertissement Ignorer le certificat** sur la page d'ouverture de session ;
- les services de Server Administrator ne sont pas activés sur le système VMware ESXi 3.5. Consultez le *Guide d'installation et de sécurité de Dell OpenManage* pour obtenir des informations sur la façon d'activer les services de Server Administrator sur le système VMware ESXi 3.5.
- le service SFCBD (small footprint CIM broker daemon) du système VMware ESXi 3.5 ne s'exécute pas.
- le service Web Server Management Service du système géré ne s'exécute pas.
- vous entrez l'adresse IP du système géré, et non le nom d'hôte, et ne cochez pas la case **Ignorer l'avertissement de certificat**.
- la fonctionnalité d'autorisation WinRM (activation distante) n'est pas configurée sur le système géré. Pour obtenir des informations sur cette fonctionnalité, consultez le *Guide d'installation et de sécurité de Dell OpenManage*.

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

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

Pour forcer une réinstallation :

1. Déterminez la version de Server Administrator installée précédemment.
2. Téléchargez le progiciel d'installation de cette version à partir du site Web de support de Dell™ **à l'adresse support.dell.com**.
3. Localisez **SysMgmt.msi** dans le répertoire **srvadmin\windows\SystemsManagement**.
4. Tapez la commande suivante à l'invite de commande pour effectuer une réinstallation forcée

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

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

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

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

Services OpenManage Server Administrator

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

Nom de service	Description	Impact de la panne	Mécanisme de récupération	Severity
Windows : service de	Fournit un accès à distance/local à Server	Les utilisateurs ne seront pas en mesure	Service de	Critique

connexion DSM SA Linux : dsm_om_connsvc (Ce service est installé avec Server Administrator Web Server.)	Administrator à partir de n'importe quel système doté d'un navigateur Web pris en charge et d'une connexion réseau.	d'ouvrir une session Server Administrator et d'effectuer une opération quelconque via l'interface utilisateur Web. Néanmoins, la CLI peut toujours être utilisée.	redémarrage	
Service commun				
Windows : services partagés DSM SA 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).	ITA ne pourra plus être utilisé pour effectuer les mises à jour de logiciels. Toutefois, celles-ci pourront être exécutées localement et hors de Server Administrator à l'aide des progiciels Dell Update Package. Les mises à jour pourront être exécutées à l'aide d'outils tiers (par exemple, MSSMS, Altiris et Novell ZENworks).	Service de redémarrage	Avertissement
Services d'instrumentation				
Windows : Gestionnaire de données DSM SA Linux : dsm_sa_datamgr32d (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 pourront pas configurer/afficher des détails sur le niveau matériel depuis l'interface GUI/CLI si ces services ne sont pas en cours d'exécution.	Service de redémarrage	Critique
Gestionnaire d'événements DSM SA (Windows) Linux : dsm_sa_eventmgr32d (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. Il est aussi utilisé par les analyseurs de journaux d'événements.	Si ce service est arrêté, les fonctions de journalisation des événements ne fonctionneront pas correctement.	Service de redémarrage	Avertissement
Linux : dsm_sa_snmp32d (hébergé sous le service dataeng) (Ce service s'exécute sur le système géré.)	Data Engine Linux SNMP Interface	Les demandes SNMP get/set /trap ne fonctionneront pas à partir d'une station de gestion.	Service de redémarrage	Critique
Storage Management Service				
Windows : mr2kserv (Ce service s'exécute sur le système géré.)	Le service Storage Management fournit des informations sur la gestion du stockage et des fonctionnalités avancées pour configurer un stockage local ou distant rattaché à un système.	Les utilisateurs ne pourront pas effectuer de fonctions de stockage pour tous les contrôleurs RAID et non-RAID pris en charge.	Service de redémarrage	Critique

Retour à la page du sommaire

Retour à la page du sommaire

Questions les plus fréquentes

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

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

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

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

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

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

   Pour les systèmes dotés de la version 4.3, aucun chemin de mise à niveau n'est requis. Pour les systèmes dotés d'une version antérieure à la version 4.3, vous devrez d'abord effectuer une mise à niveau vers la version 4.3, puis à nouveau effectuer une mise à niveau vers une version 5.x (x indique la version de Server Administrator vers laquelle vous souhaitez effectuer une mise à niveau).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Communication ITA avec les systèmes Linux :

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

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

   Communication ITA avec les systèmes Windows :

   Pour les serveurs (systèmes exécutant les systèmes d'exploitation Windows Server), le système peut être configuré avec le protocole SNMP et/ou CIM en vue de la découverte par ITA. L'inventaire nécessite CIM. Les mises à jour de logiciel, comme sous Linux, ne sont pas liées à la découverte et à l'interrogation, ni aux protocoles utilisés. À l'aide des références de niveau administrateur exigées à la période à laquelle la mise à jour est planifiée ou effectuée, un partage d'administration (lecteur) est établi sur un lecteur du système cible, et une copie de fichier(s) d'un endroit quelconque (éventuellement un autre partage réseau) est effectuée sur le système cible. Les fonctions WMI sont ensuite invoquées pour exécuter la mise à jour de logiciel.

   Pour les clients/stations de travail, Server Administrator n'est pas installé ; par conséquent, la découverte CIM est utilisée lorsque la cible exécute OpenManage Client Instrumentation. Pour de nombreux autres périphériques comme les imprimantes réseau, le protocole SNMP constitue toujours la norme pour communiquer avec (essentiellement découvrir) le périphérique. Les périphériques tels que le stockage EMC possèdent des protocoles propriétaires. Certaines informations relatives à cet environnement peuvent être recueillies en consultant les tableaux des ports utilisés dans la documentation OpenManage.

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

Non, aucun plan n'est prévu pour la prise en charge de SNMP v3 dans cette version.

10. **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 interdit. De plus, tous les autres caractères spéciaux (à l'exception du tiret) sont également interdits. Vous devez utiliser uniquement des lettres majuscules et minuscules, ainsi que des chiffres.

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

    Si vous ne cochez pas la case Active Directory, vous disposerez uniquement de l'accès configuré dans Microsoft Active Directory. Vous ne serez pas en mesure d'ouvrir une session à l'aide de la solution de schéma étendu Dell dans Microsoft® Active Directory. Cette solution vous permet de fournir l'accès à Server Administrator, et d'ajouter et ou/contrôler des utilisateurs et des privilèges de Server Administrator aux utilisateurs existants dans votre logiciel Active Directory. Pour plus d'informations, consultez la section « Utilisation de Microsoft Active Directory » du *Guide d'installation et de sécurité de Dell OpenManage*.

Retour à la page du sommaire

Retour à la page du sommaire

Glossaire

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

La liste suivante définit ou identifie les termes techniques, les abréviations et les sigles utilisés dans les documents de votre système.

authentification

Server Administrator Remote Access Controller utilise deux méthodes pour authentifier l'accès utilisateur :

L'authentification par RAC et l'authentification par le système d'exploitation local. L'authentification par RAC est toujours activée. Les administrateurs peuvent configurer des comptes utilisateurs et des mots de passe qui permettent d'accéder à RAC.

Les systèmes d'exploitation demandent aussi aux administrateurs de définir différents niveaux d'utilisateurs et de comptes d'utilisateur ; chaque niveau d'utilisateur a des privilèges différents. L'authentification par le système d'exploitation local sur RAC est l'option utilisée par les administrateurs qui ne veulent pas définir un ensemble de privilèges pour les utilisateurs du système d'exploitation et un ensemble d'utilisateurs et de comptes séparé pour RAC. Si vous activez l'authentification par le système d'exploitation local sur RAC, vous permettez à n'importe quel utilisateur avec des droits d'administrateur sur le système d'exploitation d'ouvrir une session sur RAC.

BA

Abréviation de bloc d'alimentation.

barrette de mémoire

Petite carte à circuits imprimés qui contient des puces DRAM et se connecte à la carte système.

BIOS flash

Un BIOS qui est enregistré en mémoire flash plutôt qu'en ROM. Une puce de BIOS flash peut être mise à jour sur le système, alors qu'un BIOS en ROM doit être remplacé par une nouvelle puce.

bloc d'alimentation

Un système électrique qui convertit le courant alternatif sortant de la prise murale en courant continu pour les circuits du système. Le bloc d'alimentation d'un ordinateur personnel génère plusieurs tensions.

BMC

Abréviation de Baseboard Management Controller (contrôleur de gestion de la carte mère), contrôleur qui fournit les renseignements dans la structure IPMI.

capacité

Fait référence aux actions qu'un objet peut effectuer, ou aux actions qui peuvent êtres entreprises sur un objet géré. Par exemple, si une carte est enfichable à chaud, elle peut être remplacée lorsque le système est sous tension.

carte mère

En tant que carte à circuits imprimés principale, la carte système contient en général la plupart des composants intégrés de votre système, comme :

- Microprocesseur
- RAM
- les contrôleurs des périphériques standard, comme le clavier ;
- Différentes puces ROM

Carte mère et carte logique sont des synonymes fréquemment utilisés de carte système.

Carte réseau (NIC)

Sigle de Network Interface Contrôleur (contrôleur d'interface réseau).

CEM

Abréviation de compatibilité électromagnétique.

certificat X.509

Un certificat X.509 associe une clé de cryptage publique à l'identité ou à un autre attribut de son propriétaire. Les propriétaires peuvent être des personnes, des codes d'application (tels qu'une applet signée) ou n'importe quelle autre identité identifiée de manière unique (un service de connexion DSM SA ou un serveur Web, par exemple).

CHAP

Sigle de Challenge-Handshake Authentication Protocol (protocole d'authentification Challenge Handshake), un système d'authentification utilisé par les serveurs PPP pour valider l'identité de l'origine de la connexion, quelle qu'elle soit, n'importe quand.

CIM

Sigle de Common Information Model (modèle commun d'informations), qui sert de modèle pour la description des informations de gestion du DMTF. Le CIM est indépendant de l'implémentation, ce qui permet à différentes applications de gestion de rassembler les données requises à partir d'une grande variété de sources. Le CIM inclut des schémas destinés aux systèmes, réseaux, applications et périphériques auxquels de nouveaux schémas seront ajoutés. Il fournit des techniques de mappage permettant l'échange entre les données CIM et MIB via des agents SNMP.

CLI

Abréviation de Command Line Interface (interface de ligne de commande).

CMC

Sigle de Chassis Management Controller.

contrôleur

Puce qui contrôle le transfert des données entre le microprocesseur et la mémoire ou entre le microprocesseur et un périphérique, par exemple, un lecteur de disque, le clavier.

DBPM

Abréviation de Demand Based Power Management (gestion de l'alimentation basée sur la demande).

débit en bauds

Mesure de la vitesse de transmission des données. Par exemple, les modems sont conçus pour transmettre les données à un ou plusieurs débits en bauds spécifiques par le port COM (série) d'un système.

délai d'attente

Période d'inactivité du système spécifique qui doit s'écouler avant qu'une fonction d'économie d'énergie ne soit activée.

DHCP

Abréviation de Dynamic Host Configuration Protocol (protocole de configuration dynamique de l'hôte), un protocole qui fournit un moyen d'allouer dynamiquement des adresses IP à des ordinateurs sur un réseau local.

DIMM

Sigle de Dual In-line Memory Module (module de mémoire en ligne double). Petite carte à circuits imprimés qui contient des puces DRAM et se connecte à la

carte système.

dissipateur de chaleur

Plaque métallique munie de broches et de saillies qui aident à dissiper la chaleur. La plupart des microprocesseurs sont munis d'un dissipateur de chaleur.

DMTF

Abréviation de Distributed Management Task Force, un consortium d'entreprises représentant les fournisseurs de matériels et de logiciels qui développe et tient à jour des normes relatives à la gestion de systèmes d'environnements informatiques au sein des entreprises et sur Internet.

DRAC 4

Sigle de Dell™ Remote Access Controller 4.

DRAC 5

Sigle de Dell Remote Access Controller 5.

DRAM

Abréviation de Dynamic Random-Access Memory (mémoire vive dynamique). La RAM d'un système est généralement constituée entièrement de puces DRAM. Comme les puces DRAM ne peuvent pas conserver indéfiniment une charge électrique, votre système actualise sans cesse les puces DRAM de votre système.

ECC

Abréviation de Error Checking and Correction (contrôle et correction d'erreurs).

EMI

Abréviation de ElectroMagnetic Interference (perturbation électromagnétique).

EMM

Abréviation de Expanded Memory Manager (gestionnaire de mémoire paginée). Il s'agit d'un utilitaire qui utilise la mémoire étendue pour émuler la mémoire paginée sur les systèmes dotés d'un microprocesseur Intel386™ ou supérieur.

enfichage à chaud

Permet de retirer et remplacer une pièce redondante pendant que le système est en cours d'exécution. Également appelé « remplacement à chaud ».

ERA/MC

Abréviation d'Embedded Remote Access/Modular Computer (accès distant intégré/ordinateur modulaire). Voir système modulaire.

ERA/O

Abréviation d'Embedded Remote Access Option (option d'accès distant intégré).

ERA

Abréviation d'Embedded Remote Access (accès distant intégré).

ESM

Abréviation de Embedded Systems Management (gestion de systèmes intégrés).

état

Représente la condition d'un objet qui peut en avoir plusieurs. Par exemple, un objet peut être dans un état « non prêt ».

état

Représente l'intégrité ou le fonctionnement d'un objet. Par exemple, la condition d'un capteur de température peut être normale si le capteur mesure des températures acceptables. Lorsque le capteur commence à lire des mesures qui dépassent les limites définies par l'utilisateur, il renvoie un état critique.

Fibre Channel

Interface de transfert des données intégrant des E/S haute vitesse et une fonctionnalité de mise en réseau dans une technologie de connectivité unique. La norme Fibre Channel prend en charge plusieurs topologies, y compris le point à point Fibre Channel, la structure Fibre Channel (topologie de commutation générique) et la boucle arbitrée Fibre Channel (FC_AL).

fournisseur

Un fournisseur est une extension du schéma CIM qui communique avec les objets gérés et accède aux données et aux notifications d'événements depuis une multitude de sources. Les fournisseurs font suivre ces informations au gestionnaire d'objet CIM pour les intégrer et les interpréter.

FRU

Abréviation de Field Replaceable Unit (unité remplaçable sur site).

Gigabit

Sur une carte système, les commutateurs contrôlent divers circuits ou fonctions de votre système informatique. Ces commutateurs sont appelés commutateurs DIP ; ils sont regroupés par deux ou plus dans un boîtier en plastique. Deux commutateurs DIP courants sont utilisés sur les cartes système : les commutateurs à glissière et les commutateurs à bascule. Le nom de ces commutateurs indique comment leur réglage (activé et désactivé) est effectué.

Hauteur instantanée

Elle correspond à la puissance maximale théorique consommée par le bloc d'alimentation moins la puissance instantanée consommée.

Hauteur maximale

Correspond à la puissance maximale théorique consommée par un bloc d'alimentation moins la puissance maximale consommée.

HPFS

Abréviation de l'option High Performance File System (système de fichiers ultra performant) dans le système d'exploitation Windows NT.

HTTP

Abréviation de HyperText Transfer Protocol (protocole de transfert hypertexte). Le protocole HTTP est le protocole client-serveur TCP/IP utilisé sur le Web pour l'échange de documents HTML.

HTTPS

Abréviation de HyperText Transmission Protocol, Secure (protocole de transmission hypertexte, sécurisé). Le HTTPS est une variante du HTTP utilisé par les navigateurs Web afin de traiter des transaction sécurisées. Le HTTPS est un protocole unique, avec SSL sous HTTP. Vous devez utiliser « https:// » pour les URL HTTP avec SSL, mais vous continuez à utiliser « http:// » pour les URL HTTP sans SSL.

Hyperviseur intégré

Voir *USB interne*

iDRAC

Sigle de Integrated Dell Remote Access Controller.

iDRAC6 Enterprise

Il s'agit d'une carte facultative qui contient une carte SD dédiée aux fonctionnalités avancées et qui permet d'établir une communication réseau dédiée vers iDRAC.

IP address (Adresse IP)

Abréviation d'adresse Internet Protocol (protocole Internet). Voir TCP/IP.

IPMI

Abréviation de Intelligent Platform Management Interface (interface de gestion de plate-forme intelligente), une norme de l'industrie pour la gestion de périphériques utilisés sur les ordinateurs d'entreprise basés sur l'architecture Intel. La caractéristique clé de l'IPMI, c'est que les fonctions de contrôle d'inventaire, de surveillance, de journalisation et de récupération sont disponibles, indépendamment des processeurs principaux, du BIOS et du système d'exploitation.

IPv6

Internet Protocol version 6 (protocole Internet version 6).

IRQ

Abréviation d'Interrupt ReQuest (requête d'interruption). Signal indiquant que des données vont être envoyées ou reçues par un périphérique passe au microprocesseur par une ligne d'IRQ. Chaque connexion avec un périphérique doit avoir un numéro d'IRQ. Par exemple, le premier port série de votre système (COM1) est assigné à l'IRQ4 par défaut. Deux périphériques peuvent avoir la même IRQ, mais vous ne pouvez pas utiliser ces deux périphériques simultanément.

iSCSI

Sigle de Internet SCSI. Une norme de stockage en réseau basée sur les IP pour un lien plus aisé entre les données lors du stockage. En transmettant les commandes SCSI via des réseaux en IP, iSCSI est utilisé pour faciliter les transferts de données sur les Intranets et pour gérer le stockage sur de longues distances.

JSS

Abréviation de Java™ Secure Socket Extension (extension de support Java sécurisée).

Kerberos

Protocole d'authentification de réseau. Il garantit l'authenticité d'applications client/serveur grâce à un système de cryptographie à base de clés secrètes.

LDAP

Sigle de Lightweight Directory Access Protocol (protocole léger d'accès aux annuaires). Protocole réseau de requête et de modification de services d'annuaire s'exécutant sur TCP/IP.

LPT*n*

Les noms de périphérique des trois premiers ports parallèles d'imprimante de votre système sont LPT1, LPT2 et LPT3.

LRA

Abréviation de Local Response Agent (agent de réponse local).

mémoire flash

Type de puce EEPROM qui peut être reprogrammée avec un utilitaire sur disquette tout en restant installée dans le système ; la plupart des puces EEPROM ne peuvent être réécrites qu'avec un équipement de programmation spécial.

mémoire système

Mémoire système est synonyme de RAM.

MIB

Sigle de Management Information Base (base de gestion d'informations). MIB est utilisée pour envoyer des commandes et des conditions détaillées à partir ou à un périphérique géré SNMP.

micrologiciel

Logiciels (programmes ou données) qui ont été écrits sur une mémoire morte (ROM). Le micrologiciel peut démarrer et faire fonctionner un périphérique. Chaque contrôleur contient un micrologiciel qui fournit la fonctionnalité du contrôleur.

microprocesseur

Puce de calcul principale du système qui contrôle l'interprétation et l'exécution des fonctions arithmétiques et logiques. Souvent, un logiciel écrit pour un microprocesseur doit être modifié pour pouvoir s'exécuter sur un autre microprocesseur. UC est synonyme de microprocesseur.

module de serveur

Composant de système modulaire qui fonctionne comme un système individuel. Pour fonctionner comme un système, un module de serveur est inséré dans un châssis qui inclut des blocs d'alimentation, des ventilateurs, un module de gestion de système et au moins un module de commutateur de réseau. Les blocs d'alimentation, les ventilateurs, le module de gestion du système et le module du commutateur de réseau sont des ressources partagées des modules de serveurs dans le châssis. Reportez-vous à la système modulaire.

MOF

Sigle de Managed Object Format (format d'objet géré), un fichier ASCII qui contient la définition formelle d'un schéma CIM.

nom

Le nom d'un objet ou d'une variable est la chaîne exacte qui l'identifie dans un fichier de base d'informations de gestion (MIB) SNMP ou dans un fichier objet géré (MOF) CIM.

NTFS

Abréviation de l'option Windows NT File System (système de fichiers Windows NT) dans le système d'exploitation Windows NT. NTFS est un système de fichiers avancé conçu pour être utilisé spécifiquement à l'intérieur du système d'exploitation Windows NT. Il prend en charge la récupération des systèmes de fichiers, les médias de stockage de très grande taille et les longs noms de fichiers. Il prend aussi en charge des applications orientées objet, en traitant tous les fichiers comme des objets avec des attributs définis par l'utilisateur et par le système. Voir aussi FAT et FAT32.

NTLM

Abréviation de Windows NT LAN Manager (gestionnaire de réseau local Windows NT). NTLM est le protocole de sécurité du système d'exploitation Windows NT.

NUMA

Non-Uniform Memory Architecture (architecture de la mémoire non uniforme).

OID

Abréviation de Object IDentifier (identificateur d'objet). Entier ou pointeur à implémentation qui identifie un objet de manière unique.

PAM

Sigle de Pluggable Authentication Modules (modules d'authentification enfichables). Les PAM permettent à l'administrateur système de définir des règles d'authentification sans avoir à recompiler les programmes d'authentification.

panneau de commande

Partie du système qui contient les voyants et boutons, tels que le commutateur d'alimentation, le voyant d'accès au disque dur et le voyant d'alimentation.

paramètre

Valeur ou option que vous spécifiez à un programme. Un paramètre est parfois appelé commutateur ou argument.

paramètres

Les paramètres sont les conditions d'un objet gérable et déterminent ce qui se produit lorsqu'une valeur particulière est détectée dans un composant. Par exemple, un utilisateur peut définir le seuil critique supérieur d'un capteur de température sur 75 degrés Celsius. Si la sonde atteint cette température, le paramètre déclenche une alerte qui est envoyée au système de gestion afin que l'utilisateur puisse intervenir. Certains paramètres, lorsqu'ils sont atteints, peuvent déclencher l'arrêt du système ou une autre réponse pour empêcher d'endommager le système.

partition d'utilitaires

Une partition d'amorçage sur le disque dur qui fournit des utilitaires et des diagnostics pour votre matériel et vos logiciels. Une fois activée, la partition s'amorce et fournit un environnement exécutable aux utilitaires de la partition.

PERC

Sigle de PowerEdge™ Expandable RAID controller (contrôleur RAID extensible PowerEdge™).

périphérique

Dispositif interne ou externe, tel qu'une imprimante, un lecteur de disque ou un clavier, connecté à un système.

PKCS #7

Abréviation de Public Key Cryptography Standard #7 (norme de cryptographie à clés publiques n?7). PKCS #7 est une norme de RSA Data Security, Inc. qui sert à encapsuler des données signées, comme une chaîne de certificat.

PMBus

Power Management Bus (bus de gestion de l'alimentation)

port série

Port d'E/S utilisé le plus souvent pour connecter un modem au système. Un port série se reconnaît généralement à son connecteur à 9 broches.

ppm

Abréviation de pages par minute.

PPP

Abréviation de protocole point à point.

programme de configuration du système

Programme du BIOS qui vous permet de configurer le matériel de votre système et d'en personnaliser son fonctionnement en paramétrant des fonctionnalités telles que la protection par mot de passe et la gestion de l'énergie. Certaines options du programme de configuration du système exigent que vous redémarriez le système (ou le système redémarre automatiquement) pour effectuer une modification de la configuration matérielle. Parce que le programme de configuration du système est stocké dans la mémoire NVRAM, tout paramètre reste effectif jusqu'à ce que vous le changiez.

RAC

Sigle de Remote Access Controller.

RAID

Sigle de Redundant Array of Independent Drives (matrice redondante de disques indépendants).

RBAC

Abréviation de Role-Based Access Control (contrôle d'accès basé sur le rôle).

ROM

Sigle de Read-Only Memory (mémoire morte). Votre système contient des programmes essentiels à son fonctionnement en code ROM. Contrairement à la RAM, la puce ROM garde son contenu même si le système est éteint. Le programme qui lance la procédure d'amorçage de votre système et le POST sont des exemples de code en ROM.

SAS

Acronyme de Secure Authentication Services (services d'authentification sécurisés) ou Serial-Attached SCSI (SCSI raccordé en série). Lorsqu'il est question de protocoles de sécurité ou d'authentification, SAS signifie Secure Authentication Services. Lorsqu'il est question de périphériques informatiques qui utilisent un support série (un bit à la fois) de transfert des données numériques sur des câbles fins, SAS signifie Serial-attached SCSI.

SCSI

Sigle de Small Computer System Interface (interface système pour micro-ordinateur). Interface de bus d'E/S avec des transmissions de données plus rapides que les ports standard. Vous pouvez connecter jusqu'à sept périphériques (15 pour certains types SCSI plus récents) à une interface SCSI.

SEL

Sigle de System Event Log (journal des événements système).

serveur Web

Application qui permet d'afficher les pages Web avec des navigateurs Web utilisant le protocole HTTP.

Service de connexion DSM SA

Sigle de Dell Systems Management Server Administration .Une application qui permet d'afficher les pages Web avec des navigateurs Web utilisant le protocole HTTPS. Voir « serveur Web ».

SMART

Sigle de Self-Monitoring Analysis Reporting Technology (technologie de contrôle et de prévision des performances). Technologie qui permet aux disques durs de signaler les erreurs et les pannes au BIOS du système, lequel affiche alors un message d'erreur à l'écran. Pour bénéficier de cette technologie, vous devez avoir un disque dur conforme SMART et la prise en charge appropriée dans le BIOS du système.

SMTP

Abréviation de Simple Mail Transfer Protocol (protocole de transfert de courrier simple).

SNMP

Abréviation de Simple Network Management Protocol (protocole simplifié de gestion de réseau). SNMP, un protocole commun de contrôle et de surveillance de réseau, fait partie de la première suite de protocoles TCP/IP. SNMP fournit le format dans lequel les informations vitales sur différents périphériques réseau, tels que les serveurs ou routeurs réseau, peuvent être envoyées à une application de gestion.

SSL

Abréviation de Secure Socket Layer (canal de communication sécurisé).

syntaxe

Règles selon lesquelles une commande ou une instruction doit être tapée pour être comprise par le système. La syntaxe d'une variable indique quel est son type de données.

système de gestion distant

Un système de gestion distant est tout système ayant accès à la page d'accueil de Server Administrator sur un système géré depuis un emplacement distant avec un navigateur Web pris en charge. Voir système géré.

système géré

Un système géré est tout système qui est surveillé et géré par Server Administrator. Les systèmes utilisant Server Administrator peuvent être gérés localement ou à distance via un navigateur Web pris en charge. Voir système de gestion distant.

système modulaire

Système qui peut comprendre plusieurs modules de serveurs. Chaque module de serveur fonctionne comme un système individuel. Pour fonctionner comme un système, un module de serveur est inséré dans un châssis qui inclut des blocs d'alimentation, des ventilateurs, un module de gestion de système et au moins un module de commutateur de réseau. Les blocs d'alimentation, les ventilateurs, le module de gestion du système et le module du commutateur de réseau sont des ressources partagées des modules de serveurs dans le châssis. Voir module de serveur.

système X Window

L'interface utilisateur graphique utilisée sur les distributions Linux®.

tableau

Dans les MIB SNMP, un tableau est une matrice à deux dimensions qui décrit les variables constituant un objet géré.

TCP/IP

Abréviation de Transmission Control Protocol/Internet Protocol (protocole de contrôle des transmissions/protocole Internet). Système qui permet de transférer des informations sur un réseau informatique composés de systèmes dissemblables, comme les systèmes fonctionnant sous Windows et UNIX.

TFTP

Abréviation de Trivial File Transfer Protocol (protocole de transfert de fichiers simple). TFTP est une version du protocole FTP TCP/IP qui n'a aucune capacité de répertoire ou de mot de passe.

TPM

Sigle de Trusted Platform Module (module de plateforme sécurisée).

tr/min

Abréviation de Red Hat® Package Manager.

UART

Sigle de Universal Asynchronous Receiver Transmitter (transmetteur-récepteur asynchrone universel), le circuit électronique qui constitue le port série.

unité de refroidissement

Série de ventilateurs ou d'autres périphériques de refroidissement dans le châssis d'un système.

URL

Abréviation de Uniform Resource Locator (localisateur de site uniforme [précédemment Universal Resource Locator]).

USB interne

Le lecteur flash USB interne est un périphérique de stockage supplémentaire. L'USB interne améliore les capacités de virtualisation.

USB

Abréviation de Universal Serial Bus (bus série universel). Un connecteur USB fournit un point de connexion unique pour de multiples périphériques conformes USB, comme les souris, les claviers, les imprimantes et les haut-parleurs d'ordinateur. Les périphériques USB peuvent aussi être connectés et déconnectés pendant que le système s'exécute.

utilitaire

Programme utilisé pour gérer les ressources d'un système comme, par exemple, la mémoire, les lecteurs de disque et les imprimantes.

UUID

Abréviation de Universal Unique IDentification (identification unique universelle).

valeurs de seuil

Les systèmes sont normalement équipés de divers capteurs qui surveillent la température, la tension, le courant et la vitesse des ventilateurs. Les valeurs des seuils d'un capteur spécifient les plages (valeurs minimale et maximale) qui déterminent si le capteur fonctionne dans des conditions normales, non critiques, critiques ou irrécupérables. Les valeurs de seuil prises en charge par Server Administrator sont les suivantes :

- UpperThresholdFatal
- UpperThresholdCritical
- UpperThresholdNoncritical
- Normal
- LowerThresholdNoncritical
- LowerThresholdCritical
- LowerThresholdFatal

variable

Composant d'un objet géré. Par exemple, une sonde de température possède une variable pour décrire ses capacités, son intégrité ou sa condition, et certains index que vous pouvez utiliser pour vous aider à repérer la bonne sonde de température.

VRM

Abréviation de Voltage Regulator Module (module régulateur de la tension).

Wh

Abréviation de wattheure.

WMI

Sigle de Windows Management Instrumentation (infrastructure de gestion Windows). WMI fournit les services de gestionnaire d'objet CIM.

Xen

Xen est un moniteur de machine virtuelle destiné aux systèmes x86.

XMM

Abréviation de eXtended Memory Manager (gestionnaire de mémoire étendue), un utilitaire qui permet aux programmes d'application et aux systèmes

d'exploitation d'utiliser la mémoire étendue conformément à XMS.

XMS

Abréviation de eXtended Memory Specification (spécification de mémoire étendue).

ZIF

Sigle de Zero Insertion Force (sans force d'insertion). Certains systèmes utilisent des supports et des connecteurs ZIF qui permettent d'installer ou de retirer des périphériques comme la puce du microprocesseur sans imposer de contrainte au périphérique.

ZIP

Lecteur de disque amovible de 3,5 pouces développé par Iomega. À l'origine, il offrait des cartouches amovibles de 100 Mo. Le lecteur dispose de logiciels qui peuvent cataloguer les disques et verrouiller les fichiers pour plus de sécurité. Une version 250 Mo du lecteur Zip peut également procéder à la lecture et à l'écriture des cartouches Zip de 100 Mo.

Retour à la page du sommaire

Retour à la page du sommaire

Services Server Administrator

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

Présentation

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

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

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

REMARQUE : Pour les systèmes gérés et stations de gestion réseau fonctionnant sous Microsoft® Windows Server® 2003, vous devez configurer le service SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]) pour qu'il accepte les paquets SNMP. Voir « Configuration de l'agent SNMP pour les systèmes fonctionnant sous un système d'exploitation Windows pris en charge » pour obtenir des informations détaillées.

Gestion de votre système

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

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

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

REMARQUE : Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. En cliquant sur **Aide** sur la barre de navigation globale, vous pouvez ouvrir une fenêtre d'aide indépendante contenant des informations détaillées sur la fenêtre spécifique que vous consultez. L'aide en ligne est conçue pour vous donner des conseils spécifiques sur les actions à prendre pour mener à bien toutes les phases des services de Server Administrator. L'aide en ligne est disponible pour toutes les fenêtres que vous pouvez consulter, en fonction des groupes logiciels et matériels que Server Administrator découvre sur votre système et de votre niveau de privilèges d'utilisateur.

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

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

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

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

Pour des informations détaillées sur le composant Storage Management Service, consultez le Guide d'utilisation de*Dell OpenManage Server Administrator Storage Management* disponible sur le DVD *Dell Systems Management tools and Documentation* ou sur le site web du support de Dell à l'adresse **support.dell.com**.

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

Fonctionnalités non prises en charge dans OpenManage Server Administrator

En raison des limitations du système d'exploitation VMware ESXi, version 3.5 et 4.0, certaines fonctionnalités disponibles dans les versions antérieures d'OpenManage Server Administrator ne sont pas disponibles dans la présente version. Il s'agit des fonctionnalités suivantes :

Fonctionnalités non prises en charge d'OM 6.1 sur ESXi 3.5

- Gestion des alertes - Actions d'alerte
- Configuration du BIOS - Séquence d'amorçage (*systèmes xx1x*)
- Configuration du BIOS - Sécurité du module de plate-forme sécurisée (TPM)
- Interface réseau - Condition d'administration
- Interface réseau - DMA (Direct Memory Access [accès direct à la mémoire])
- Interface réseau - Adresse du protocole Internet (IP)
- Interface réseau - Adresse MAC
- Interface réseau - Unité de transmission maximale
- Interface réseau - Condition opérationnelle
- Gestion de l'alimentation - Profils (*systèmes xx1x*)
- Préférences - Configuration SNMP
- Processeurs - Capacités - Commutation à la demande (DBS) (*systèmes xx1x*)
- Arrêt distant - Système de cycle d'alimentation avec arrêt du SE en premier

Fonctionnalités non prises en charge d'OM 6.1 sur ESXi 4.0

- Gestion des alertes - Actions d'alerte
- Interface réseau - Condition d'administration
- Interface réseau - DMA (Direct Memory Access [accès direct à la mémoire])
- Interface réseau - Adresse du protocole Internet (IP)
- Interface réseau - Adresse MAC
- Interface réseau - Unité de transmission maximale
- Interface réseau - Condition opérationnelle
- Gestion de l'alimentation - Profils (*systèmes xx1x*)
- Préférences - Configuration SNMP
- Processeurs - Capacités - Commutation à la demande (DBS) (*systèmes xx1x*)
- Arrêt distant - Système de cycle d'alimentation avec arrêt du SE en premier

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

Enceinte modulaire

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

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

Propriétés

Sous-onglets : Information

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 créer un lien vers la fenêtre **Ouvrir une session** de Chassis Management Controller depuis la page d'accueil de Server Administrator, cliquez sur l'objet **Enceinte modulaire**, cliquez sur l'onglet **Informations sur CMC**, puis cliquez sur **Lancer l'interface Web de CMC**. La fenêtre **Ouvrir une session** de CMC

apparaît. Une fois connecté à CMC , vous pouvez surveiller et gérer votre enceinte modulaire.

Système/Module de serveur

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

REMARQUE : La fonctionnalité de mise à jour est prise en charge sur Server Administrator version 2.0 ou antérieure. Dell™ Server Update Utility et les progiciels Dell Update Package peuvent être téléchargés à partir du site Web de support de Dell à l'adresse **support.dell.com**. Ils sont pris en charge sur les systèmes d'exploitation Microsoft Windows®, Red Hat® Enterprise Linux® et SUSE® Linux Enterprise Server.

REMARQUE : Dell Server Update Utility ou les progiciels Dell Update Package doivent être lancés à partir du système que vous voulez mettre à jour.

Propriétés

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

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

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

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

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

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

Arrêt

Sous-onglets : Arrêt distant | Arrêt thermique | Arrêt du serveur Web

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

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

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

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

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

Journaux

Sous-onglets : Matériel | Alerte | Commande

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

- Afficher le journal de gestion de système intégrée (ESM) ou le journal d'événements du système (SEL) pour voir une liste de tous les événements associés aux composants matériels de votre système. L'icône de condition à côté du nom du journal passera d'une condition normale () à une condition non critique () lorsque le fichier journal atteint une capacité de 80 %. Sur les systèmes Dell™ PowerEdge™ *x8xx*, *x9xx et* xx1x, l'icône indicateur de condition située en regard du nom du journal se transforme en condition critique ( ) lorsque le fichier journal atteint une capacité de 100 %.

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

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

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

- Afficher le journal des commandes pour voir 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 : Voir « Journaux de Server Administrator » pour des instructions détaillées sur l'affichage, l'impression, l'enregistrement et l'envoi par e-mail des journaux.

Gestion des alertes

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

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

- Voir 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.
- Voir tous les paramètres actuels des filtres d'événements de plateforme et définir les actions de filtrage d'événements de plateforme à effectuer si le capteur d'un composant du système donne une valeur d'avertissement ou de panne. Vous pouvez également utiliser l'option **Configurer la destination** pour sélectionner une destination (adresse IPv4 ou IPv6) vers laquelle une alerte concernant un événement sur plateforme sera envoyée.

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

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

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

Gestion des sessions

Sous-onglets : Session

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

- Voir 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 voir la page Gestion des sessions et mettre fin aux sessions des utilisateurs connectés.

Châssis principal du système/Système principal

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

Les composants disponibles sont :

- Piles
- BIOS
- Ventilateurs
- Micrologiciel
- Performances matérielles
- Intrusion
- Mémoire
- Réseau
- Ports
- Power Management
- Blocs d'alimentation
- Processeurs
- Accès à distance
- Logements
- Températures
- Tensions

REMARQUE : **Performances du matériel** est pris en charge uniquement sur les systèmes Dell *xx0x*.

REMARQUE : **Blocs d'alimentation** n'est pas disponible sur le système Dell PowerEdge *1900*.

REMARQUE : **Gestion de l'alimentation** est pris en charge sur des systèmes Dell *xx0x* limités.

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

Propriétés.

Propriétés

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

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

- Voir l'intégrité ou la condition des composants matériels et des capteurs. Chaque composant répertorié a une icône « Indicateurs de condition des composants de système/module de serveur » à côté de son nom. Une coche verte ( ) indique que le composant est en bon état (normal). Un triangle jaune avec un point d'exclamation ( ) indique que le composant est dans un état d'avertissement (non critique) et requiert une intervention rapide. Un X rouge ( ) indique que le composant est dans une condition de panne (critique) et requiert une intervention immédiate. Un espace vide ( ) indique que la condition d'intégrité du composant n'est pas connue. Les composants surveillés disponibles sont :
  - Ventilateurs
  - Journal du matériel
  - Intrusion
  - Mémoire
  - Réseau
  - Power Management
  - Blocs d'alimentation
  - Processeurs
  - Températures
  - Tensions

  REMARQUE : Commutateur en CA est pris en charge sur des systèmes limités.

  REMARQUE : Batteries est pris en charge uniquement sur les systèmes Dell PowerEdge *x9xx* et Dell *xx0x* .

  REMARQUE : Blocs d'alimentation n'est pas disponible sur le système Dell PowerEdge *1900*.

  REMARQUE : Gestion de l'alimentation est pris en charge sur des systèmes Dell *xx0x* limités.

- Afficher les informations sur les attributs du châssis principal du système.
- Afficher des informations détaillées concernant les unités remplaçables sur site (FRU) installées sur votre système (sous le sous-onglet **Composants système (FRU)**.)
- Activer ou désactiver les boutons du panneau avant du système géré, à savoir le bouton d'alimentation et le bouton d'interruption non masquable (NMI) (s'il y en a un sur le système).

Commutateur de CA

Cliquez sur l'objet **Commutateur de CA** pour afficher les fonctionnalités principales du commutateur de basculement de CA de votre système. La fenêtre d'action de l'objet **Commutateur de CA** peut avoir l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, vous pouvez voir les informations sur la redondance du commutateur de CA et sur les lignes d'alimentation en CA.

Piles

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

Propriétés

Sous-onglet : Informations

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

Gestion des alertes

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

BIOS

Cliquez sur l'objet **BIOS** pour gérer les fonctionnalités clés du BIOS de votre système. Le BIOS de votre système contient des programmes, enregistrés sur un chipset de mémoire flash, qui contrôlent les communications entre le microprocesseur et les périphériques comme, par exemple, le clavier et la carte vidéo, et

d'autres fonctions diverses, telles que les messages du système. La fenêtre d'action de l'objet **BIOS** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Configuration**.

Propriétés

Sous-onglet : Informations

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

Configuration

Sous-onglet : BIOS

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

REMARQUE : La définition de la séquence d'amorçage sur **Device List** dans l'onglet **Configuration** génère la séquence d'amorçage suivante : diskette, IDE CD drive, hard drive, option ROMs (si les périphériques sont disponibles).

Vous pouvez modifier l'état des nombreuses fonctionnalités de configuration du BIOS, dont notamment le Serial Port, les cartes de Network Interface Controller, Boot Sequence, User Accessible USB Ports, CPU Virtaulization Technology, CPU HyperThreading, AC Power Recovery Mode, Embedded SATA Controller, Console Redirection et Console Redirection Failsafe Baud Rate. Vous pouvez également configurer un internal USB device, les paramètres du Trusted Platform Module (TPM), les paramètres du optical drive controller, automatic system recovery(ASR) Watchdog Timer, embedded hypervisor et des informations supplémentaires sur les ports réseau local sur la carte-mère.

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

REMARQUE : Les informations portant sur la configuration des NIC dans l'écran de configuration du **BIOS** de Server Administrator peuvent être inexactes pour les NIC intégrés. L'utilisation de l'écran de configuration du **BIOS** pour activer ou désactiver les NIC peut produire des résultats inattendus. Nous vous conseillons d'effectuer toutes les configurations des NIC intégrés dans l'écran **Configuration du système** ; vous pouvez y accéder en appuyant sur <F2> au démarrage du système.

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

Ventilateurs

Cliquez sur l'objet **Ventilateurs** pour gérer les ventilateurs de votre système. Server Administrator surveille la condition de chaque ventilateur du système en mesurant le nombre de tours/minute de chaque ventilateur. Les sondes des ventilateurs fournissent le nombre de tours/minute des ventilateurs à Server Administrator Instrumentation Service. Lorsque vous sélectionnez **Ventilateurs** dans l'arborescence de périphérique, des détails apparaissent dans la zone de données du volet de droite de la page d'accueil de Server Administrator. La fenêtre d'action de l'objet **Ventilateurs** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglets : Sondes des ventilateurs | **Contrôle des ventilateurs**

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

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

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

- Sélectionner les options de contrôle des ventilateurs.

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

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

Micrologiciel

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

Propriétés

Sous-onglet : Informations

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

Performances matérielles

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

Tableau 5-1 répertorie les valeurs possibles pour la condition et la cause d'une sonde :

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

Propriétés

Sous-onglet : Informations

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

Intrusion

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

Propriétés

Sous-onglet : Intrusion

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

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

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

Mémoire

Cliquez sur l'objet **Mémoire** pour gérer les périphériques de mémoire de votre système. Server Administrator surveille la condition des périphériques de mémoire pour chaque module de mémoire installé sur le système surveillé. Les capteurs de panne anticipée des périphériques de mémoire surveillent les modules de mémoire en comptant le nombre de corrections de mémoire ECC. Server Administrator surveille aussi les informations sur la redondance de mémoire si cette fonctionnalité est prise en charge par votre système. La fenêtre d'action de l'objet **Mémoire** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés et Gestion des alertes**.

Propriétés

Sous-onglet : Mémoire

Sous l'onglet **Propriétés**, vous pouvez afficher les attributs de la mémoire, les détails sur les périphériques de mémoire et leur condition.

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

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

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

Réseau

Cliquez sur l'objet **Réseau** pour gérer les NIC de votre système. Server Administrator surveille la condition de chaque NIC installé sur votre système pour assurer une connexion à distance ininterrompue. La fenêtre d'action de l'objet **Réseau** peut avoir l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, vous pouvez voir les informations sur les NIC installés sur votre système.

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

Ports

Cliquez sur l'objet **Ports** pour gérer les ports externes de votre système. Server Administrator surveille la condition de chaque port externe présent sur votre système. La **fenêtre** d'action de l'objet Ports peut avoir l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

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

Power Management

Analyse

Sous-onglets : Consommation | **Statistiques**

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

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

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

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

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

Gestion

Sous-onglets : Bilan | **Profils**

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

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

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

Utilisez l'onglet Interruptions SNMP pour configurer les interruptions SNMP de votre système.

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

Blocs d'alimentation

Cliquez sur l'objet Blocs d'alimentation pour gérer les blocs d'alimentation de votre système. Server Administrator surveille la condition des blocs d'alimentation, y compris la redondance, pour assurer que les blocs d'alimentation installés sur votre système fonctionnent correctement. La fenêtre d'action de l'objet Blocs d'alimentation peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglet : Éléments

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

- Voir les informations sur les attributs de redondance de vos blocs d'alimentation.
- Vérifier la condition des blocs d'alimentation individuels, y compris la puissance d'entrée nominale et la puissance de sortie maximale. L'attribut de puissance d'entrée nominale s'affiche uniquement sur les systèmes PMBus à partir de la version *xx1x*.

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

- Voir 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.
- Voir les seuils actuels d'alerte des interruptions SNMP et définir les niveaux des seuils d'alerte des watts d'alimentation du système. Les interruptions sélectionnées seront déclenchées si le système génère un événement correspondant au niveau de gravité sélectionné.

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

Processeurs

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

Propriétés

Sous-onglet : Informations

Sous l'onglet **Propriétés**, vous pouvez voir 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 | **Interruptions SNMP**

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

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

Accès à distance

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

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

REMARQUE : Le **contrôleur BMC** est pris en charge par les systèmes Dell PowerEdge *x8xx* et *x9xx*, et le contrôleur **iDRAC est pris en charge par les systèmes Dell** *xx0x* ***et*** *xx1x* uniquement.

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

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

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

Propriétés

Sous-onglet : Informations

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

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

Configuration

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

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

Sous l'onglet **Configuration,** lorsque le contrôleur DRAC est configuré, vous pouvez :

- Configurer les propriétés du réseau

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

Sous l'onglet Configuration supplémentaire, vous serez en mesure d'activer ou de désactiver les propriétés IPv4/IPv6.

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

Utilisateurs

Sous-onglet : Utilisateurs

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

REMARQUE : Sur les systèmes Dell PowerEdge *x9xx* :

- Dix ID d'utilisateur s'affichent. Si une carte DRAC est installée, seize ID d'utilisateur s'affichent.
- La colonne Charge utile de la connexion série sur le réseau local s'affiche.

Logements

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

Propriétés

Sous-onglet : Informations

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

Températures

Cliquez sur l'objet **Températures** pour gérer la température de votre système afin d'éviter l'endommagement thermique de ses composants internes. Server Administrator surveille la température à plusieurs endroits du châssis de votre système pour que les températures dans le châssis ne soient pas trop élevées. La fenêtre d'action de l'objet **Températures** peut avoir les onglets suivants, selon les privilèges de groupe de l'utilisateur : **Propriétés** et **Gestion des alertes**.

Propriétés

Sous-onglet : Sondes de température

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

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

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

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

REMARQUE : Les utilisateurs ne peuvent définir les valeurs minimales et maximales des seuils des sondes de température pour un châssis externe que sur des nombres entiers. Si les utilisateurs essaient de définir la valeur minimale ou maximale des seuils des sondes de température sur un nombre décimal, seul le nombre entier avant la virgule est enregistré comme paramètre de seuil.

Tensions

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

Propriétés

Sous-onglet : Sondes de tension

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

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

Gestion des alertes

Sous-onglets : Actions d'alerte | **Interruptions SNMP**

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

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

Logiciels

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

Propriétés

Sous-onglet : Résumé

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

Système d'exploitation

Cliquez sur l'objet **Système d'exploitation** pour voir des informations de base sur votre système d'exploitation. La fenêtre d'action de l'objet **Système d'exploitation** comporte l'onglet suivant, selon les privilèges de groupe de l'utilisateur : **Propriétés**.

Propriétés

Sous-onglet : Informations

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

Stockage

Server Administrator fournit Storage Management Service :

Storage Management Service offre des fonctionnalités pour la configuration des périphériques de stockage. Dans la plupart des cas, Storage Management Service est installé à l'aide de l'option Installation rapide. Storage Management Service est disponible sur les systèmes d'exploitation Microsoft Windows, Red Hat Enterprise Linux et SUSE® Linux Enterprise Server.

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

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

Propriétés

Sous-onglet : Intégrité

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

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

Le panneau gauche de la page d'accueil Préférences (là où s'affiche l'arborescence du système sur la page d'accueil de Server Administrator) affiche toutes les options de configuration disponibles dans la fenêtre de l'arborescence du système. Les options affichées sont fonction du logiciel Systems Management installé sur le système géré.

Voir Tableau 5-2 pour les options de configuration disponibles de la page d'accueil Préférences.

Tableau 5-2. Options de configuration de la page d'accueil Préférences

⊟	.....	Paramètres généraux
⊟	.....	Server Administrator

Paramètres généraux

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

Utilisateur

Sous-onglet : Propriétés

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

Serveur Web

Sous-onglets : Propriétés | **Certificat X.509**

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

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

Server Administrator

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

Préférences

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

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

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

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

- Configurer les opérations Set SNMP.

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

Retour à la page du sommaire

Retour à la page du sommaire

Introduction

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

Présentation

Server Administrator fournit une solution de gestion de systèmes un-à-un complète, qui peut être utilisée de deux façons : depuis une interface utilisateur graphique (IUG) intégrée faisant appel à un navigateur Web ou depuis une interface de ligne de commande (CLI) via le système d'exploitation. Cette version prend également en charge les systèmes VMware® ESXi 3.5 et ESXi 4.0. Server Administrator a été conçu pour les administrateurs système afin qu'ils puissent gérer les systèmes localement et à distance sur un réseau. Il permet aux administrateurs système de se concentrer sur la gestion de l'ensemble de leur réseau grâce à une gestion de systèmes un-à-un complète.

Server Administrator peut être utilisé avec un système autonome, un système ayant des unités de stockage réseau connectées dans un châssis séparé ou un système modulaire composé d'un ou plusieurs modules de serveur dans une enceinte modulaire.

Server Administrator fournit des informations sur :

- Les systèmes qui fonctionnent correctement et ceux qui sont défectueux
- Les systèmes qui requièrent des opérations de récupération à distance.

Fonctionnalités intégrées

Server Administrator permet de gérer et d'administrer facilement des systèmes locaux et distants via une série complète de services de gestion intégrés. Server Administrator est le seul à être installé sur le système géré et est accessible à la fois localement et à distance depuis la page d'accueil de Server Administrator. Les systèmes surveillés à distance sont accessibles par connexions par réseau commuté, LAN ou sans fil. Server Administrator assure la sécurité de ses connexions de gestion par contrôle d'accès basé sur le rôle (RBAC), l'authentification et le cryptage standard de l'industrie SSL.

Installation

Vous pouvez installer Server Administrator à l'aide du DVD *Dell Systems Management Tools and Documentation*. Le DVD contient un programme de configuration pour installer, mettre à niveau et désinstaller Server Administrator, ainsi que les autres composants logiciels Managed System Software sur votre système géré. Ce DVD comprend également un programme de configuration pour installer, mettre à niveau et désinstaller les composants logiciels Management Station sur votre station de gestion. Vous pouvez également installer Server Administrator sur plusieurs systèmes en réalisant une installation automatique sur un réseau.

Le programme d'installation de Dell™ OpenManage™ fournit des scripts d'installation et des paquetages RPM pour installer et désinstaller Dell OpenManage Server Administrator et d'autres composants du logiciel Managed System sur votre système géré. Pour plus d'informations, consultez le *Guide d'installation et de sécurité de Dell OpenManage,* et le *Guide d'installation rapide du logiciel Dell OpenManage*. Vous pouvez accéder à ces documents sur le DVD *Dell Systems Management Tools and Documentation* ou sur le site web du support de Dell à l'adresse **support.dell.com**.

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

Mise à jour de composants système particuliers

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

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

Storage Management Service

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

Pour obtenir des informations détaillées sur Storage Management Service, consultez le *Guide d'utilisation de Dell OpenManage Server Administrator Storage Management* disponible sur le *DVD Dell Systems Management tools and Documentation* **ou s**ur le site web du support de Dell à l'adresse support.dell.com.

Instrumentation Service

Instrumentation Service fournit un accès rapide à des informations détaillées sur les défaillances et les performances recueillies par des agents de gestion de

systèmes standard de l'industrie et permet l'administration à distance de systèmes surveillés, y compris l'arrêt, le démarrage et la sécurité.

Remote Access Controller

REMARQUE : Remote Access Controller n'est pas disponible sur des systèmes modulaires. Vous devez vous connecter directement au contrôleur Dell Embedded Remote Access/Modular Chassis (ERA/MC) sur un système modulaire. Consultez le *Guide d'utilisation de l'accès à distance intégré /MC de Dell* pour des informations supplémentaires.

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

Journaux

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

Page d'accueil de Server Administrator

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

Autres documents utiles

Outre ce *Guide d'utilisation*, vous pouvez trouver les guides suivants sur le site web du support de Dell à l'adresse **support.dell.com** ou sur le DVD *Dell Systems Management Tools and Documentation* :

- La *matrice de prise en charge logicielle des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- Le *Guide d'installation et de sécurité de Dell OpenManage* fournit des informations complètes sur les procédures d'installation et des instructions détaillées pour l'installation, la mise à niveau et la désinstallation de Server Administrator sur les systèmes d'exploitation pris en charge.
- Le *Guide d'installation rapide du logiciel Dell OpenManage* présente les applications que vous pouvez installer sur votre station de gestion (la console) et vos systèmes gérés, ainsi que les procédures d'installation de votre console et des applications de systèmes gérés sur des systèmes exécutant des systèmes d'exploitation pris en charge.
- Le *Guide de compatibilité de Dell OpenManage Server Administrator* fournit des informations de compatibilité sur l'installation et le fonctionnement de Server Administrator sur diverses plates-formes matérielles (ou systèmes) exécutant des systèmes d'exploitation Microsoft Windows, Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge.
- Le *Guide de référence SNMP de Dell OpenManage Server Administrator* fournit des informations sur la base d'informations de gestion (MIB) du protocole SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]). La MIB SNMP définit les variables qui étendent la MIB standard pour couvrir les capacités des agents de gestion de systèmes.
- Le *Guide de référence CIM de Dell OpenManage Server Administrator* répertorie le fournisseur du modèle commun d'informations (CIM), une extension du fichier de format d'objet de gestion standard (MOF). Le fichier MOF du fournisseur CIM détaille les classes d'objets de gestion prises en charge.
- Le *Guide de référence des messages de Dell OpenManage Server Administrator* répertorie les messages qui s'affichent dans votre journal des alertes de la page d'accueil de Server Administrator ou sur l'afficheur d'événements de votre système d'exploitation. Ce guide explique le texte, la gravité et la cause de chaque message d'alerte d'Instrumentation Service émis par Server Administrator.
- Le *Guide d'utilisation de l'interface de ligne de commande de Dell OpenManage Server Administrator* fournit des informations sur l'interface de ligne de commande complète de Server Administrator, y compris l'explication des commandes CLI pour l'affichage des conditions du système, l'accès aux journaux, la création de rapports, la configuration de différents paramètres de composants et la définition de seuils critiques.
- Le *Guide d'utilisation de Dell Integrated Remote Access Controller* fournit des informations détaillées sur la configuration et l'utilisation du contrôleur iDRAC.
- Le *Guide d'utilisation de Dell Chassis Management Controller* fournit des informations détaillées sur l'installation, la configuration et l'utilisation du contrôleur CMC.
- Le *Guide d'utilisation de Dell Online Diagnostics* fournit des informations complètes sur l'installation et l'utilisation de Online Diagnostics sur votre système.
- Le *Guide d'utilisation de Dell OpenManage Baseboard Management Controller Utilities* fournit des informations supplémentaires sur l'utilisation de Server Administrator pour configurer et gérer le contrôleur BMC de votre système.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator Storage Management* est un guide de référence complet pour la configuration et la gestion du stockage local et distant connecté à un système.
- Le *Guide d'installation et de configuration de Dell Remote Access Controller* fournit des informations détaillées sur l'installation et la configuration d'un DRAC III, d'un DRAC III/XT ou d'un contrôleur ERA/O, la configuration d'un contrôleur ERA et l'utilisation d'un RAC pour accéder à distance à un système inutilisable.
- Le *Guide d'utilisation de l'utilitaire Racadm de Dell Remote Access Controller* fournit des informations sur l'utilisation de l'utilitaire de ligne de commande racadm.
- Le *Guide d'utilisation de Dell Remote Access Controller 4* fournit des informations complètes sur l'installation et la configuration d'un contrôleur DRAC 4 et son utilisation pour accéder à distance à un système ne fonctionnant pas.

- Le *Guide d'utilisation de Dell Remote Access Controller 5* fournit des informations complètes sur l'installation et la configuration d'un contrôleur DRAC 5 et son utilisation pour accéder à distance à un système ne fonctionnant pas.
- Le *Guide d'utilisation de Dell Embedded Remote Access/MC Controller* fournit des informations complètes sur la configuration et l'utilisation d'un contrôleur ERA/MC pour gérer et contrôler à distance votre système modulaire et ses ressources partagées sur un réseau.
- Le *Guide d'utilisation de Dell OpenManage Remote Install* fournit des informations sur les solutions de configuration et de dimensionnement automatiques et simultanées sur le réseau par l'utilisation d'une technologie basée image.
- Le *Guide d'utilisation des progiciels Dell Update Packages* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Packages dans le cadre de votre stratégie de mise à jour du système.
- Consultez le *Guide d'utilisation de Dell OpenManage Server Update Utility* pour plus d'informations sur la manière d'obtenir et d'utiliser Server Update Utility (SUU) pour mettre à jour vos systèmes Dell ou pour afficher les mises à jour disponibles pour n'importe quel système répertorié dans la logithèque.
- Le *Guide d'utilisation de Dell Management Console* contient des informations sur l'installation, la configuration et l'utilisation de Dell Management Console. Dell Management Console est un logiciel de gestion de systèmes Web qui vous permet de détecter et d'inventorier les périphériques présents sur votre réseau. Il fournit également des fonctions avancées, comme par exemple la surveillance de l'intégrité et des performances des périphériques mis en réseau et des capacités de gestion de correctifs pour les systèmes Dell.

Le DVD *Dell Systems Management Tools and Documentation* contient un fichier « Lisez-moi » pour Server Administrator, ainsi que la plupart des applications figurant sur ce DVD.

Obtention d'une assistance technique

Si vous ne comprenez pas une procédure décrite dans ce guide ou si votre produit ne fonctionne pas comme prévu, des outils d'aide sont disponibles pour vous assister. Pour des informations supplémentaires sur ces outils d'aide, voir « Obtention d'aide » du *Manuel du propriétaire de matériel* de votre système.

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

Retour à la page du sommaire

Retour à la page du sommaire

Journaux de Server Administrator

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

Présentation

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

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

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

Fonctionnalités intégrées

Cliquez sur un en-tête de colonne pour trier d'après cette colonne ou changer l'ordre de tri de la colonne. De plus, chaque fenêtre de journal contient plusieurs boutons de tâche qui permettent de gérer et de prendre en charge votre système.

Boutons de tâche des fenêtres des journaux

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

Voir « Boutons de tâche » pour des informations supplémentaires sur l'utilisation des boutons de tâche.

Journaux de Server Administrator

Server Administrator fournit les journaux suivants :

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

Journal du matériel

Utilisez le journal du matériel pour détecter les problèmes éventuels des composants matériels de votre système. Sur les systèmes Dell PowerEdge™ *x8xx*, *x9xx et xx1x*, l'indicateur de condition du journal du matériel se transforme en condition critique () lorsque le fichier journal atteint une capacité de 100 %. Deux journaux du matériel sont disponibles selon votre système : le journal de gestion système intégrée (ESM) et le journal des événements système (SEL). Les journaux ESM et SEL contiennent chacun un jeu d'instructions intégrées qui peuvent envoyer des messages sur la condition du matériel au logiciel de gestion de systèmes. Chaque composant répertorié dans les journaux comporte une icône d'indicateur de condition à côté de son nom. Une coche verte () indique que le composant est en bon état (normal). Un triangle jaune avec un point d'exclamation ( ) indique que le composant est dans un état d'avertissement (non critique) et requiert une intervention rapide. Un X rouge () indique que le composant est dans un état de panne (critique) et requiert une intervention immédiate. Un espace vide () indique que la condition d'intégrité du composant n'est pas connue.

Pour accéder au journal du matériel, cliquez sur **Système**, puis sur l'onglet **Journaux** et sur **Matériel**.

Les informations affichées dans les journaux ESM et SEL comprennent :

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

Maintenance du journal du matériel

L'icône de l'indicateur de condition à côté du nom du journal dans la page d'accueil de Server Administrator passera d'une condition normale ( ) à une condition non critique ( ) lorsque le fichier journal aura atteint une capacité de 80 %. Effacez le journal du matériel lorsqu'il a atteint une capacité de 80 %. Si le journal atteint une capacité de 100 %, les événements les plus récents ne sont pas journalisés.

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 sur le journal.

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

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

Les informations affichées sur 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
- Une description de l'événement

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

Consultez le *Guide de référence des messages de Server Administrator* pour des informations détaillées sur les messages d'alerte.

Journal de commandes

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

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

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

Les informations affichées sur le journal de commandes comprennent :

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

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

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de Remote Access Controller

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

REMARQUE : Le **contrôleur de gestion de la carte mère (BMC)** est pris en charge par *les systèmes* Dell™ *P*owerEdge™ *x8xx et* x9xx, et le contrôleur **Integrated Dell Remote Access Controller (iDRAC)** est pris en charge par les systèmes Dell *xx0x* et *xx1x*.

Présentation

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

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

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

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

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

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

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

REMARQUE : Consultez le Guide d'utilisation de *Dell OpenManage*™ BaseBoard Management Controller Utilities pour des informations supplémentaires sur le contrôleur BMC.

REMARQUE : Consultez le *Guide d'utilisation de Dell Remote Access Controller 4* pour plus d'informations sur l'utilisation de DRAC 4 ou le *Guide d'utilisation de Dell Remote Access Controller 5* pour plus d'informations sur l'utilisation de DRAC 5.

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

Tableau 6-1 répertorie les noms des champs de l'IUG et le système concerné, lorsque Server Administrator est installé sur le système.

Tableau 6-1. Disponibilité du système pour les noms des champs de l'IUG suivants

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

Consultez la *matrice de prise en charge des logiciels système Dell* pour plus d'informations sur la prise en charge des systèmes concernant les périphériques d'accès à distance.

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

- Afficher les informations de base
- Configurer le périphérique d'accès à distance sur une connexion LAN

- Configurer le périphérique d'accès à distance sur une connexion par communication série sur le LAN
- Configurer le périphérique d'accès à distance sur une connexion par port série
- Configurer des propriétés de périphérique d'accès à distance supplémentaires
- Configurer des utilisateurs sur le périphérique d'accès à distance
- Définir des alertes de filtre d'événements sur 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 plateforme (PEF) et les destinations d'alerte.

REMARQUE : Vous pouvez consulter les données du contrôleur BMC sur les systèmes Dell PowerEdge *x8xx* et *x9xx* uniquement.

Affichage des informations de base

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

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

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

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

   Périphérique d'accès à distance

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

   Adresse IPv4

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

   Adresse IPv6

   - Source d'adresse IP
   - Adresse 1 IPv6
   - Passerelle par défaut
   - Adresse 2 IPv6
   - Adresse locale du lien
   - Source d'adresse DNS
   - Serveur DNS préféré
   - Serveur DNS secondaire

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

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

REMARQUE : Les champs **Configuration du réseau local** sont affichés en lecture seule s'ils sont configurés comme *disabled* pour les utilisateurs intrabande.

Vous pouvez configurer le périphérique d'accès à distance en vue d'établir une communication sur le LAN . Pour ce faire :

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

   La fenêtre **Configuration du réseau local** s'affiche.

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

4. Spécifiez les détails de configuration du NIC suivants :

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

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

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

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

   - Sélection de NIC

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

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

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

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

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

6.
7. 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 secondaire

REMARQUE : Vous serez 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

Vous pouvez configurer le contrôleur BMC pour les communications sur un port série. Pour ce faire :

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

   La fenêtre **Configuration du port série** apparaît.
4. Configurez les détails suivants :
   - Paramètre du mode de connexion
   - Débit en bauds
   - Contrôle du flux
   - Limite du niveau de privilège du canal
5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur **Paramètres du mode terminal**.

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

   Le mode terminal est utilisé pour la messagerie IPMI (gestion de l'interface de plate-forme intelligente) sur le port série à l'aide de caractères ASCII imprimables. Le mode terminal prend aussi en charge un nombre limité de commandes texte pour prendre en charge les environnements classiques basés sur texte. Cet environnement est conçu pour qu'un terminal simple ou un émulateur de terminal puisse être utilisé.
7. Spécifiez les personnalisations suivantes pour accroître la compatibilité avec les terminaux existants :
   - Modification de ligne
   - Contrôle de la suppression
   - Contrôle d'écho
   - Contrôle de la négociation
   - Nouvelle séquence linéaire
   - Saisie d'une nouvelle séquence linéaire
8. Cliquez sur **Appliquer les modifications**.
9. Cliquez sur **Retourner à la fenêtre Configuration du port série** pour revenir à la fenêtre **Configuration du port série**.

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

Vous pouvez configurer les contrôleurs BMC/iDRAC pour les communications série sur le réseau local (SOL). Pour ce faire :

1. Cliquez sur l'objet **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Connexion série sur le réseau local**.

   La fenêtre **Configuration de la connexion série sur le réseau local** apparaît.
4. Configurez les détails suivants :
   - Activer la connexion série sur le réseau local

- Débit en bauds
- Privilèges minimum requis

5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur **Paramètres avancés** pour configurer le contrôleur BMC.
7. Dans la fenêtre **Paramètres avancés de la configuration de la connexion série sur le réseau local**, vous pouvez spécifier les informations suivantes :
   - Intervalle d'accumulation des caractères
   - Seuil d'envoi des caractères
8. Cliquez sur **Appliquer les modifications**.
9. Cliquez sur **Retourner à la configuration de la connexion série sur le réseau local** pour revenir à la fenêtre **Configuration de la connexion série sur le réseau local**.

Configuration supplémentaire pour iDRAC

Vous pouvez configurer les propriétés IPv4 et IPv6 via l'onglet Configuration supplémentaire. Pour ce faire :

1. Cliquez sur l'objet **Enceinte modulaire→ Système/Module de serveur→ Châssis principal du système/Système principal→ Accès à distance**.
2. Cliquez sur l'onglet **Configuration**.
3. Cliquez sur **Configuration supplémentaire.**
4. Configurez les propriétés IPv4 et IPv6 en les définissant sur **Activé** ou **Désactivé.**
5. Cliquez sur **Appliquer les modifications**.

Configuration des utilisateurs du périphérique d'accès à distance

Vous pouvez configurer les utilisateurs du périphérique d'accès à distance via la page **Accès à distance**. Pour accéder à cette page :

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

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

   La fenêtre **Configuration des utilisateurs de l'accès à distance** vous permet de configurer un utilisateur des contrôleurs BMC/iDRAC spécifique.
4. Spécifiez les informations générales suivantes :
   - Sélectionnez **Activer l'utilisateur** pour activer l'utilisateur.
   - Entrez le nom de l'utilisateur dans le champ **Nom d'utilisateur**.
   - Sélectionnez la case à cocher **Modifier le mot de passe**.
   - Entrez un nouveau mot de passe dans le champ **Nouveau mot de passe**.
   - Entrez encore le nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe**.
5. Spécifiez les privilèges d'utilisateur suivants :
   - Sélectionnez la limite maximale de privilèges utilisateur sur le réseau local.
   - Sélectionnez la limite maximale de privilèges utilisateur sur le port série accordée.
   - Sur les systèmes Dell PowerEdge *x9xx*, sélectionnez Activer la connexion série sur le réseau local pour activer la connexion série sur le réseau local.
6. Spécifiez le groupe d'utilisateurs pour les privilèges d'utilisateur des contrôleurs DRAC/iDRAC.
7. Cliquez sur **Appliquer les changements** pour enregistrer les modifications.

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

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

Définition des alertes de filtre d'événements sur plateforme

Vous pouvez utiliser Server Administrator Instrumentation Service pour configurer les fonctionnalités du contrôleur BMC les plus importantes, comme les paramètres de filtre d'événements de plate-forme (PEF) et les destinations d'alerte. Pour ce faire :

1. Cliquez sur l'objet **Système**.

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

3. Cliquez sur **Événements sur plate-forme**.

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

   REMARQUE : Vous devez être connecté avec des privilèges d'administrateur pour pouvoir configurer les alertes de filtre d'événements de plate-forme du contrôleur BMC.

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

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

   REMARQUE : Sur les systèmes Dell PowerEdge 1900, les filtres d'événements de plate-forme **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 plate-forme pour lequel vous voulez effectuer des actions d'arrêt ou générer des alertes pour les actions sélectionnées et cliquez sur **Définir des événements de plate-forme**.

   La fenêtre **Définir des événements de plate-forme** vous permet de spécifier les actions à entreprendre si le système doit être arrêté en réponse à un événement de plate-forme.

5. Sélectionnez l'une des actions suivantes :

   - **None (Aucun)**
     Ne réagit pas si le système d'exploitation est bloqué ou qu'il tombe en panne.
   - **Redémarrer le système**
     Arrête le système d'exploitation et initialise un démarrage du système, en effectuant les vérifications du BIOS et en rechargeant le système d'exploitation.
   - **Effectuer un cycle d'alimentation système**
     Met le système hors tension, attend brièvement, le remet sous tension et le redémarre. Le cycle d'alimentation est utile si vous voulez réinitialiser des composants système comme, par exemple, les disques durs.
   - **Mettre le système hors tension**
     Met le système hors tension.
   - **Baisse de l'alimentation**
     Accélère l'UC.

PRÉCAUTION : Si vous sélectionnez une action d'arrêt d'événement de plate-forme autre que Néant ou Baisse de l'alimentation, un arrêt forcé de votre système s'effectuera lorsque l'événement spécifié se produira. Cet arrêt est mis en ouvre par le micrologiciel et est effectué sans arrêter d'abord le système d'exploitation ou toute application en cours d'exécution.

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

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

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

8. Cliquez sur **Retourner à la page Événements de plate-forme** pour revenir à la fenêtre **Filtres d'événements de plate-forme**.

Définition des destinations des alertes d'événements de plate-forme

Vous pouvez également utiliser la fenêtre **Filtres d'événements de plate-forme** pour sélectionner une destination vers laquelle une alerte concernant une plate-forme sera envoyée. En fonction du nombre de destinations qui s'affichent, vous pouvez configurer une adresse IP différente pour chaque adresse de

destination. Une alerte d'événement de plate-forme sera envoyée à chaque adresse IP de destination que vous configurez.

1. Cliquez sur **Configurer les destinations** dans la fenêtre **Filtres d'événements de plate-forme.**

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

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

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

3. Sélectionnez la case à cocher **Activer la destination**.

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

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

6. Cliquez sur **Appliquer les modifications**.

7. Cliquez sur **Retourner à la page Événements de plate-forme** pour revenir à la fenêtre **Filtres d'événements de plate-forme**.

Retour à la page du sommaire

Retour à la page du sommaire

Configuration et administration

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

Gestion de la sécurité

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

Contrôle de l'accès basé sur le rôle

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

Privilèges d'utilisateur

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

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

Server Administrator accorde l'accès en lecture seule aux utilisateurs connectés avec des privilèges *utilisateur*, l'accès en lecture et en écriture aux utilisateurs connectés avec des droits d'*utilisateur privilégié*, et l'accès en lecture, en écriture et d'administrateur aux utilisateurs connectés avec des privilèges d'*administrateur* et d'*administrateur élevé*. Voir Tableau 3-1.

Tableau 3-1. Privilèges d'utilisateur

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

Niveaux de privilèges pour accéder aux services de Server Administrator

Tableau 3-2 résume quels niveaux d'utilisateurs ont des privilèges d'accès et de gestion pour les services de Server Administrator.

Tableau 3-2. Niveaux de privilèges d'utilisateur de Server Administrator

Service	Niveau de privilège d'utilisateur requis	
	Vue	Gérer
Instrumentation	U, P, A, EA	P, A, EA
Accès à distance	U, P, A, EA	A, EA

Gestion de stockage	U, P, A, EA	A, EA

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

Tableau 3-3. Légende pour les niveaux de privilège d'utilisateur de Server Administrator

U	Utilisateur
P	Utilisateur privilégié
A	Administrateur
EA	Administrateur élevé

Authentification

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

Authentification Microsoft Windows

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

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

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

REMARQUE : L'authentification de Server Administrator à l'aide de Winbind et Kerberos sur SUSE Linux Enterprise Server (version 9, Service Pack 3) n'est pas prise en charge car les bibliothèques compatibles 32 bits pour Winbind et Kerberos ne font pas partie de ce système d'exploitation.

Cryptage

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

Attribution des privilèges d'utilisateur

Pour garantir la sécurité des composants critiques du système, attribuez des privilèges d'utilisateur à tous les utilisateurs du logiciel Dell™ OpenManage™ avant d'installer le logiciel Dell OpenManage. Les nouveaux utilisateurs peuvent ouvrir une session sur le logiciel Dell OpenManage avec les privilèges d'utilisateur de leur système d'exploitation.

PRÉCAUTION : Pour protéger l'accès aux composants critiques de votre système, vous devez attribuer un mot de passe à chaque compte d'utilisateur qui a accès au logiciel Dell OpenManage. Les utilisateurs qui n'ont pas de mot de passe attribué ne peuvent pas se connecter au logiciel Dell OpenManage sur un système exécutant Windows Server 2003 en raison de la conception du système d'exploitation.

PRÉCAUTION : Désactivez les comptes d'invités sur les systèmes d'exploitation Windows pris en charge afin de protéger l'accès à vos composants système critiques. Pensez à renommer les comptes pour que les scripts distants ne puissent pas activer les comptes en utilisant le nom.

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

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

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

REMARQUE : Vous devez avoir installé Microsoft Active Directory® sur votre système pour pouvoir effectuer les procédures suivantes. Voir « Microsoft Active Directory » pour des informations supplémentaires sur l'utilisation d'Active Directory.

1. Naviguez vers **Panneau de configuration**→ **Outils d'administration**→ **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, cliquez-droite sur **Utilisateurs** ou sur le conteneur auquel vous voulez ajouter le nouvel utilisateur et pointez sur

Nouveau→ Utilisateur.

3. Tapez les informations appropriées concernant le nom d'utilisateur dans la boîte de dialogue et cliquez sur **Suivant**.
4. Cliquez sur **Suivant** et cliquez ensuite sur **Terminer**.
5. Double-cliquez sur l'icône représentant l'utilisateur que vous venez de créer.
6. Cliquez sur l'onglet **Membre de**.
7. Cliquez sur **Add (Ajouter)**.
8. Sélectionnez le groupe approprié et cliquez sur **Ajouter**.
9. Cliquez sur **OK** et cliquez ensuite une deuxième fois sur **OK**.

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

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

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

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

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

Création d'utilisateurs

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

Création d'utilisateurs avec des privilèges d'utilisateur

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

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

   où `<groupe>` n'est *pas* `root`.

   REMARQUE : Si `<groupe>` n'existe pas, vous devez le créer en vous servant 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 qui a accès à Server Administrator pour protéger l'accès aux composants critiques de votre système.

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

Création d'utilisateurs avec des privilèges d'utilisateur privilégié

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

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

   REMARQUE : Vous devez définir `root` comme le 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 qui a accès à Server Administrator pour protéger l'accès aux composants critiques de votre système.

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

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

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

1. Ouvrez le fichier **omarolemap** situé à l'emplacement **/etc**.
2. Ajoutez la ligne suivante au fichier :

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

   Tableau 3-4 répertorie les légendes concernant l'ajout de la définition du rôle au fichier *omarolemap*

Tableau 3-4. Légendes concernant l'ajout de la définition du rôle dans OpenManage Server Administrator

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

Tableau 3-5 répertorie les exemples concernant l'ajout de la définition du rôle au fichier *omarolemap*

Tableau 3-5. Exemples concernant l'ajout de la définition du rôle dans OpenManage Server Administrator

<Nom_d'utilisateur>	<Nom_d'hôte>	<Droits>
Bob	Ahôte	Utilisateur privilégié
+root	Bhôte	Administrateur
+root	Chôte	Administrateur
Bob	*.aus.amer.com	Utilisateur privilégié
Mike	192.168.2.3	Utilisateur privilégié

3. Enregistrez les modifications et fermez le fichier.
4. Exécutez la commande suivante depuis la ligne de commande pour redémarrer le service de connexion :

   ```
   service dsm_om_connsvc restart
   ```

REMARQUE : Vérifiez que vous redémarrez bien le service de connexion pour que vos modifications deviennent effectives.

Meilleures pratiques pendant l'utilisation du fichier omarolemap

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

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

root	*	Administrateur
+root	*	Utilisateur privilégié
*	*	Utilisateur

- Ne modifiez pas les permissions ou le format du fichier **omarolemap.**
- Server Administrator utilise le privilège d'utilisateur par défaut du système d'exploitation si un utilisateur est dégradé dans le fichier **omarolemap**.
- N'utilisez pas l'adresse de retour de boucle pour *<Nom_d'hôte>*, par exemple : hôte local ou 127.0.0.1.
- Lorsque les services de connexion ont été redémarrés et que les modifications ne sont pas effectives pour le fichier **/etc/omarolemap**, consultez le journal des commandes pour prendre connaissance des erreurs.

- Lorsque le fichier **omarolemap** est copié d'un ordinateur à un autre, les permissions et les entrées du fichier doivent être revérifiées.
- Ajoutez le préfixe + au *Nom du groupe*.
- Server Administrator utilise les privilèges d'utilisateur par défaut du système d'exploitation en cas d'entrées doubles des noms d'utilisateur ou des groupes d'utilisateurs ayant le même *<Nom_d'hôte>*.
- *Espace* peut également être utilisé comme délimiteur pour les colonnes au lieu de [Tab]

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

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

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

   Un X entouré d'un cercle rouge apparaît sur le nom d'utilisateur. Le compte est désactivé.

Configuration de l'agent SNMP

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

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

REMARQUE : La configuration par défaut de l'agent SNMP comprend généralement un nom de communauté SNMP tel que **public**. Pour des raisons de sécurité, ne gardez pas les valeurs par défaut des noms de communauté SNMP. Pour des informations sur la manière de changer les noms de communauté SNMP, reportez-vous à la section correspondante ci-dessous. Pour des consignes supplémentaires, lisez l'article **Securing an SNMP Environment** (Sécurisation d'un environnement SNMP) du magazine Dell Power Solutions du mois de mai 2003. Vous pouvez trouver ce magazine sur le site **www.dell.com/powersolutions**.

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

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

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

- "Configuration de l'agent SNMP pour les systèmes fonctionnant sous un système d'exploitation Windows pris en charge"
- "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 un système d'exploitation SUSE Linux Enterprise Server pris en charge"

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

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

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

Activation de l'accès SNMP par les hôtes distants

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

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

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

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

Changement du nom de communauté SNMP

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

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

   La fenêtre **Propriétés de service SNMP** apparaît.
5. Cliquez sur l'onglet **Sécurité** pour ajouter ou modifier un nom de communauté.
   a. Pour ajouter un nom de communauté, cliquez sur **Ajouter** dans la liste **Noms de communauté acceptés**.

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

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

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

   c. Pour modifier un nom de communauté, sélectionnez un nom de communauté dans la liste **Noms de communauté acceptés** et cliquez sur **Modifier**.

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

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

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

Activation des opérations Set SNMP

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

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

4. Faites défiler la liste de services jusqu'à ce que vous trouviez **Service SNMP**, cliquez-droite sur **Service SNMP** et cliquez sur **Propriétés.**

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

5. Cliquez sur l'onglet **Sécurité** pour modifier les droits d'accès d'une communauté.

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

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

7. Définissez les **Droits de communauté** sur **LECTURE-ÉCRITURE** ou sur **LECTURE-CRÉATION** et cliquez sur OK.

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

8. Cliquez sur **OK** pour enregistrer les modifications.

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

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

1. Ouvrez la fenêtre **Gestion de l'ordinateur**.

2. Développez l'icône **Gestion de l'ordinateur** dans la fenêtre au besoin.

3. Développez l'icône **Services et applications** et cliquez sur **Services**.

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

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

5. Cliquez sur l'onglet **Interruptions** pour ajouter une communauté d'interruptions ou pour ajouter une destination d'interruption à une communauté d'interruption.

   a. Pour ajouter une communauté d'interruptions, tapez le nom de la communauté dans la boîte **Nom de la communauté** et cliquez sur **Ajouter à la liste**, à côté de la boîte **Nom de la communauté.**

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

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

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

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

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

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

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

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

Configuration du contrôle d'accès de l'agent SNMP

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

Pour les systèmes d'exploitation Red Hat Enterprise Linux, la configuration de l'agent SNMP par défaut donne un accès en lecture seule à la branche « système » MIB-II (identifiée par l'OID 1.3.6.1.2.1.1) de l'arborescence MIB pour la communauté « public ». Cette configuration ne permet pas aux applications de gestion de récupérer ou de changer Server Administrator ou d'autres informations sur la gestion de systèmes hors de la branche « système » MIB-II.

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

Si Server Administrator détecte la configuration SNMP par défaut pendant l'installation, il tente de modifier la configuration de l'agent SNMP pour fournir un accès en lecture seule à toute l'arborescence MIB pour la communauté « public ». Server Administrator modifie le fichier de configuration de l'agent

SNMP **/etc/snmp/snmpd.conf** de deux manières.

Le premier changement consiste à créer un affichage de toute l'arborescence MIB en ajoutant la ligne suivante si elle n'existe pas encore :

```
view all included .1
```

Le second changement consiste à modifier la ligne d'« accès » par défaut pour offrir un accès en lecture seule à toute l'arborescence MIB pour la communauté « public ». Server Administrator cherche la ligne suivante :

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

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

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

Ces changements apportés à la configuration de l'agent SNMP par défaut offrent un accès en lecture seule à toute l'arborescence MIB pour la communauté « public ».

REMARQUE : Afin de garantir que Server Administrator est capable de modifier la configuration de l'agent SNMP pour fournir un accès approprié aux données de gestion de systèmes, il est recommandé que tout autre changement de configuration de l'agent SNMP soit effectué après avoir installé Server Administrator.

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

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Changement du nom de communauté SNMP

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

Pour modifier le nom de communauté SNMP utilisé pour récupérer les informations de gestion depuis un système exécutant Server Administrator, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmp/snmpd.conf**) et procédez comme suit :

1. Trouvez la ligne :

   ```
   com2sec publicsec default public
   ```

   ou

   ```
   com2sec notConfigUser default public
   ```

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

   ```
   com2sec publicsec default nom_de_communauté
   ```

   ou

   ```
   com2sec notConfigUser default nom_de_communauté
   ```

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

   ```
   service snmpd restart
   ```

Activation des opérations Set SNMP

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

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

1. Trouvez la ligne :

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

   ou

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

2. Modifiez cette ligne en remplaçant le premier `none` par `all`. Une fois modifiée, la nouvelle ligne est la suivante :

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

ou

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

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

```
service snmpd restart
```

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

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

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

1. Ajoutez la ligne suivante au fichier :

   ```
   trapsink adresse_IP nom_de_communauté
   ```

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

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

   ```
   service snmpd restart
   ```

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

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

REMARQUE : Sous SUSE Linux Enterprise Server (version 10), le fichier de configuration de l'agent SNMP se trouve sous /etc/snmp/snmpd.conf.

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

Actions d'installation de Server Administrator SNMP

Server Administrator SNMP communique avec l'agent SNMP utilisant le protocole de multiplexage SNMP (SMUX). Quand Server Administrator SNMP se connecte à l'agent SNMP, il envoie un identificateur d'objet à l'agent SNMP pour s'identifier en tant qu'homologue SMUX. Cet identifiant d'objet doit être configuré avec l'agent SNMP ; Server Administrator ajoute donc la ligne suivante au fichier de configuration de l'agent SNMP (**/etc/snmpd.conf** ou **/etc/snmp/snmpd.conf**) pendant l'installation si elle n'existe pas :

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

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

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

REMARQUE : Pour des raisons de sécurité, il est recommandé 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/snmpd.conf** ou **/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Trouvez la ligne :

   ```
   rocommunity public 127.0.0.1
   ```

2. Modifiez ou copiez cette ligne, en remplaçant 127.0.0.1 par l'adresse IP de l'hôte distant. Une fois modifiée, la nouvelle ligne est la suivante :

   ```
   rocommunity public adresse_IP
   ```

   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/snmpd.conf** ou **/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Trouvez la ligne :

   ```
   rocommunity public 127.0.0.1
   ```

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

   ```
   rocommunity public
   ```

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

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

Changement du nom de communauté SNMP

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

Pour modifier le nom de communauté SNMP par défaut utilisé pour récupérer les informations de gestion depuis un système exécutant Server Administrator, modifiez le fichier de configuration de l'agent SNMP (**/etc/snmpd.conf** ou **/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Trouvez la ligne :

   ```
   rocommunity public 127.0.0.1
   ```

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

   ```
   rocommunity nom_de_communauté 127.0.0.1
   ```

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

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

Activation des opérations Set SNMP

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

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

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

1. Trouvez la ligne :

   ```
   rocommunity public 127.0.0.1
   ```

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

   ```
   rwcommunity public 127.0.0.1
   ```

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

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

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

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

Pour configurer le système exécutant Server Administrator pour qu'il envoie des interruptions à une station de gestion, modifiez le fichier de configuration de

l'agent SNMP (**/etc/snmpd.conf** ou **/etc/snmp/snmpd.conf**) et effectuez les étapes suivantes :

1. Ajoutez la ligne suivante au fichier :

   ```
   trapsink adresse_IP nom_de_communauté
   ```

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

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

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

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

Si vous sélectionnez une sécurité par pare-feu lorsque vous installez Red Hat Enterprise Linux/SUSE Linux, le port SNMP de toutes les interfaces réseau externes est fermé par défaut. Pour que des applications de gestion SNMP, comme IT Assistant, puissent découvrir et extraire des informations de Server Administrator, le port SNMP doit être ouvert sur au moins l'une des interfaces réseau externes. Si Server Administrator détecte que le port SNMP n'est pas ouvert dans le pare-feu des interfaces réseau externes, Server Administrator affiche un message d'avertissement et journalise un message dans le journal du système.

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

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

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

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

   Le menu **Choisir un outil** apparaît.

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

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

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

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

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

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

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

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

5. Sélectionnez s'il faut ouvrir toute l'interface réseau ou seulement le port SNMP de toutes les interfaces réseau.

   a. Pour ouvrir toute une interface réseau, appuyez sur <Tab> pour sélectionner un des périphériques approuvés et appuyez sur la barre d'espace. Un astérisque dans la case à gauche du nom du périphérique indique que toute l'interface sera ouverte.

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

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

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

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

   Le menu **Choisir un outil** apparaît.

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

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

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

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

3. Exécutez la combinaison de touches « Alt+d » pour ouvrir la boîte de dialogue **Ports autorisés supplémentaires**.
4. Exécutez la combinaison de touches « Alt+T » pour déplacer le curseur dans la zone de texte **Ports TCP**.
5. Entrez « snmp » dans la zone de texte.
6. Exécutez la combinaison de touches « Alt-O » et « Alt-N » pour accéder à l'écran suivant.
7. Exécutez la combinaison de touches « Alt-A » pour accepter et appliquer les modifications.

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de Server Administrator

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

---

Ouverture de votre session Server Administrator

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

L'écran **Ouvrir une session Server Administrator** apparaît. Le port par défaut de Dell™ OpenManage™ Server Administrator est 1311. Vous pouvez modifier le port, si nécessaire. Voir « Service de connexion Dell Systems Management Server Administration et configuration de la sécurité » pour des instructions sur la configuration de vos préférences système.

Ouverture et fermeture de session

Cette version d'OpenManage Server Administrator propose trois types d'ouverture de session. Les voici :

- Ouverture d'une session Server Administrator sur le système local
- Ouverture d'une session Server Administrator Managed System
- Ouverture d'une session Server Administrator Web Server

Ouverture d'une session Server Administrator sur le système local

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

Utilisez cette fenêtre d'ouverture de session pour ouvrir une session Server Administrator sur un système local :

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

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

2. Si votre système exécute un système d'exploitation Microsoft Windows tout en étant membre du domaine Windows, sélectionnez un domaine dans la liste des domaines.

3. Cochez la case Ouverture d'une session Active Directory pour ouvrir une session avec Microsoft® Active Directory®. Voir « Utilisation de l'ouverture de session Active Directory. »

4. Cliquez sur **OK**.

Pour mettre fin à votre session Server Administrator, cliquez sur le bouton **Fermer la session**, en haut à droite de chaque page d'accueil de Server Administrator.

REMARQUE : Consultez le Guide d'installation et de sécurité d'OpenManage pour obtenir des informations sur la configuration d'Active Directory sur les systèmes ne possédant pas de CLI.

Ouverture d'une session Server Administrator Managed System

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

Méthode 1

1. Cliquez sur l'icône **Dell™ OpenManage™ Server Administrator** de votre bureau.

2. Tapez vos **Nom d'hôte/Adresse IP, Nom d'utilisateur** et **Mot de passe** du système géré dans les champs appropriés de la fenêtre **Ouverture d'une session** de système de gestion distant. Si nécessaire, vous pouvez également entrer le nom de l'ordinateur ou son nom de domaine complet (FQDN) dans le champ **Nom d'hôte/Adresse IP**.

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

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

5. Cliquez sur **OK**.

Méthode 2

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

`https://nomd'hôte:1311`

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

`ou`

`https://adresse IP:1311`

où `adresse IP` est l'adresse IP du système géré et `1311` le numéro de port par défaut

Vous devez taper `https://` (et non `http://`) dans le champ d'adresse pour recevoir une réponse valide dans votre navigateur.

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

Ouverture d'une session Server Administrator Web Server

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

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

2. Cliquez sur le lien **Gérer Web Server** qui se trouve dans le coin supérieur droit de l'écran.

3. Entrez les **Nom d'utilisateur**, **Mot de passe** et **Nom de domaine** (si vous accédez à Server Administrator à partir d'un domaine défini) et cliquez sur **OK**.

4. Cochez la case **Ouverture d'une session Active Directory** pour ouvrir une session avec Microsoft® Active Directory®. Voir « Utilisation de l'ouverture de session Active Directory. »

5. Cliquez sur **OK.**

REMARQUE : Vous ne serez pas en mesure de gérer un système géré Windows à partir d'un Server Administrator Web Server Linux.

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

REMARQUE : Lorsque vous lancez Server Administrator via Internet Explorer® version 7.0, une page d'avertissement intermédiaire peut s'afficher pour indiquer un problème avec le certificat de sécurité. Pour garantir la sécurité du système, nous vous conseillons vivement de générer un nouveau certificat X.509, de réutiliser un certificat X.509 existant ou d'importer un certificat racine ou une chaîne de certificat d'une autorité de certification (CA). Pour éviter que ces messages d'avertissement sur le certificat ne s'affichent, le certificat utilisé doit être émis par une CA fiable. Pour plus d'informations sur la gestion du certificat X.509, voir « Gestion du certificat X.509 ».

Utilisation de l'option Ignorer le certificat

L'écran d'ouverture de session intègre une « case à cocher Ignorer les avertissements de certificat ».

PRÉCAUTION : Vous devez utiliser l'option « Ignorer les avertissements de certificat » avec prudence. Il est fortement recommandé de l'utiliser uniquement dans les environnements Intranet sécurisés. Pour garantir la sécurité du système, Dell vous recommande fortement d'importer un certificat racine ou une chaîne de certificat d'une autorité de certification (CA). Reportez-vous à la documentation de VMware pour plus de détails.

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

Utilisation de l'ouverture de session Active Directory

Vous devez cocher la case « Ouverture d'une session Active Directory » pour ouvrir une session à l'aide de la solution de schéma étendu Dell dans Microsoft® Active Directory.

Cette solution vous permet d'accorder l'accès à Server Administrator, et d'ajouter et/ou de contrôler les utilisateurs et les privilèges de Server Administrator aux utilisateurs existants dans votre logiciel Active Directory. Pour plus d'informations, consultez la section « Utilisation de Microsoft Active Directory » du *Guide d'installation et de sécurité de Dell OpenManage*.

Connexion directe

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

REMARQUE : Consultez l'article de la base de connaissances sur **http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258063** pour plus d'informations sur la connexion directe.

Pour accéder à l'ordinateur local, il est nécessaire d'avoir un compte sur cet ordinateur avec des privilèges appropriés (utilisateur, utilisateur privilégié ou administrateur). Les autres utilisateurs sont authentifiés avec Microsoft Active Directory.

Pour lancer Server Administrator en utilisant l'authentification par connexion directe au lieu de Microsoft Active Directory, ajoutez les paramètres suivants à :

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

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

Par exemple :

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

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

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

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

Par exemple :

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

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

Systèmes fonctionnant sous un système d'exploitation Microsoft Windows Server 2003 pris en charge

Vous devez configurer les paramètres de sécurité de votre navigateur pour ouvrir une session sur Server Administrator depuis un système de gestion distant qui fonctionne sous un système d'exploitation Microsoft Windows Server® 2003 pris en charge.

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

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

Internet Explorer

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

   Pour Windows 2000 :

   - Sous **Divers**, sélectionnez le bouton radio **Permettre l'actualisation meta**.
   - Sous **Scripts actifs**, sélectionnez le bouton radio **Activer**.

   Pour Windows 2003 :

   - Sous **Divers**, sélectionnez le bouton radio **Permettre l'actualisation meta**.

- Sous **Scripts actifs**, sélectionnez le bouton radio **Activer**.
- Sous **Scripts actifs**, sélectionnez le bouton radio **Permettre les scripts des commandes de navigation Web d'Internet Explorer**.

6. Cliquez sur **OK** pour sauvegarder les nouveaux paramètres. Fermez le navigateur et ouvrez une session Server Administrator.

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

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

Mozilla

1. Démarrez votre navigateur.
2. Cliquez sur **Modifier**→ **Préférences**.
3. Cliquez sur **Avancés**→ **Scripts et plug-ins**.
4. Assurez-vous que la case à cocher **Navigateur** est sélectionnée sous **Activer JavaScript pour**.
5. Cliquez sur **OK** pour sauvegarder les nouveaux paramètres.
6. Fermez le navigateur.
7. Ouvrez une session sur Server Administrator.

Page d'accueil de Server Administrator

REMARQUE : N'utilisez pas les boutons de la barre d'outils de votre navigateur Web (comme **Précédent** et **Actualiser**) lorsque vous utilisez Server Administrator. N'utilisez que les outils de navigation de Server Administrator.

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

- Barre de navigation globale fournit des liens vers des services généraux.
- Arborescence du système affiche tous les objets système visibles en fonction des privilèges d'accès de l'utilisateur.
- Fenêtre d'action affiche les actions de gestion disponibles pour l'objet de l'arborescence du système sélectionné en fonction des privilèges d'accès de l'utilisateur. La fenêtre d'action contient trois zones opérationnelles :
  - Les onglets d'action affichent les actions principales ou les catégories d'action qui sont disponibles pour l'objet sélectionné en fonction des privilèges d'accès de l'utilisateur.
  - Les onglets d'action sont divisés en sous-catégories comportant toutes les options secondaires disponibles pour les onglets d'action en fonction des privilèges d'accès de l'utilisateur.
  - Zone de données affiche des informations sur l'objet de l'arborescence du système sélectionné, l'onglet d'action et la sous-catégorie en fonction des privilèges d'accès de l'utilisateur.

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

Tableau 4-1 répertorie les noms des champs de l'IUG et le système concerné, lorsque Server Administrator est installé sur le système.

Tableau 4-1. Disponibilité du système pour les noms des champs de l'IUG suivants

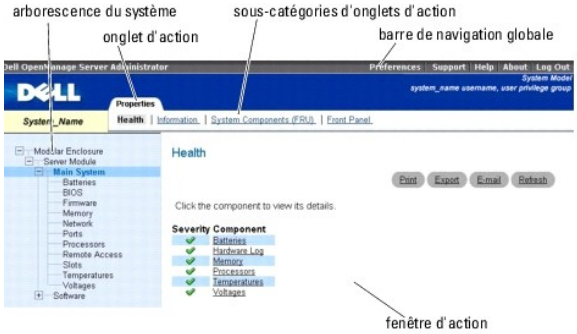
Nom de champ de l'IUG	Système concerné
Enceinte modulaire	Système modulaire
Module de serveur	Système modulaire
Système principal	Système modulaire
Système	Système non modulaire
Châssis principal du système	Système non modulaire

Figure 4-1 illustre un exemple de page d'accueil de Server Administrator pour un utilisateur ayant ouvert une session avec des privilèges d'administrateur sur un système non modulaire.

Figure 4-1. Exemple de page d'accueil de Server Administrator - Système non modulaire

Figure 4-2 illustre un exemple de page d'accueil de Server Administrator pour un utilisateur ayant ouvert une session avec des privilèges d'administrateur sur un système modulaire.

Figure 4-2. Exemple de page d'accueil de Server Administrator - Système modulaire



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

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

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

Le tableau suivant répertorie la disponibilité des fonctionnalités de Server Administrator au sein des systèmes modulaires et non modulaires. Une marque de graduation indique la disponibilité, tandis qu'une croix indique la non disponibilité de la fonctionnalité.

Fonctionnalités	Système modulaire	Système non modulaire
Piles	✓	✓
Blocs d'alimentation	✘	✓
Ventilateurs	✘	✓

Performances matérielles	✘	✓ **(à partir de la version *xx0x* du système)**
Intrusion	✘	✓
Mémoire	✓	✓
Réseau	✓	✓
Ports	✓	✓
Power Management	✓	✓ **(à partir de la version *xx0x* du système)**
Processeurs	✓	✓
Accès à distance	✓	✓
Logements	✓	✓
Températures	✓	✓
Tensions	✓	✓
Enceinte modulaire (Informations sur le châssis et sur CMC)	✓	✘

Barre de navigation globale

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

- Cliquez sur **Préférences** pour ouvrir la page d'accueil **Préférences**. Voir « Utilisation de la page d'accueil Préférences ».
- Cliquez sur **Support** pour vous connecter au site Web de support de Dell.
- Cliquez sur **Aide** pour ouvrir la fenêtre d'aide en ligne contextuelle. Voir « Utilisation de l'aide en ligne ».
- Cliquez sur **À propos** pour afficher les informations de version et de copyright de Server Administrator.
- Cliquez sur **Fermer la session** pour fermer la session du programme Server Administrator en cours.

Arborescence du système

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

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

Fenêtre d'action

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

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

Zone de données

La zone de données se situe sous les onglets d'action sur le côté droit de la page d'accueil. La zone de données vous permet d'effectuer des tâches ou d'afficher des détails sur des composants du système. Le contenu de la fenêtre dépend de l'objet de l'arborescence du système et de l'onglet d'action sélectionnés. Par exemple, si vous sélectionnez **BIOS** dans l'arborescence du système, l'onglet **Propriétés** est sélectionné par défaut et les informations sur la version du BIOS du système apparaissent dans la zone de données. La zone de données de la fenêtre d'action contient un grand nombre de fonctionnalités courantes, notamment les indicateurs de condition, les boutons de tâche, les éléments soulignés et les indicateurs de niveau.

Indicateurs de condition des composants de système/module de serveur

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

Tableau 4-2. Indicateurs de condition des composants de système/module de serveur

	Une coche verte indique que le composant est en bon état (normal).
	Un triangle jaune avec un point d'exclamation indique que le composant a une condition d'avertissement (non critique). Une condition d'avertissement se produit lorsqu'une sonde ou un autre outil de surveillance détecte une mesure sur un composant qui atteint certaines valeurs minimales ou maximales. Une condition d'avertissement exige une intervention rapide.
	Un X rouge indique que le composant est dans une condition de panne (critique). Une condition critique se produit lorsqu'une sonde ou un autre outil de surveillance détecte une mesure sur un composant qui atteint certaines valeurs minimales ou maximales. Une condition critique exige une intervention immédiate.
	Un espace vide indique que la condition d'intégrité du composant n'est pas connue.

Boutons de tâche

La plupart des fenêtres ouvertes à partir de la page d'accueil de Server Administrator contiennent au moins quatre boutons de tâche : **Imprimer**, **Exporter**, **E-mail** et **Actualiser**. D'autres boutons de tâche sont inclus dans des fenêtres particulières de Server Administrator. Les fenêtres de journaux, par exemple, contiennent également les boutons de tâche **Enregistrer sous** et **Effacer le journal**. Pour des informations spécifiques sur chaque bouton de tâche, cliquez sur **Aide** dans une fenêtre de la page d'accueil de Server Administrator pour afficher des informations détaillées sur la fenêtre particulière que vous affichez.

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

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

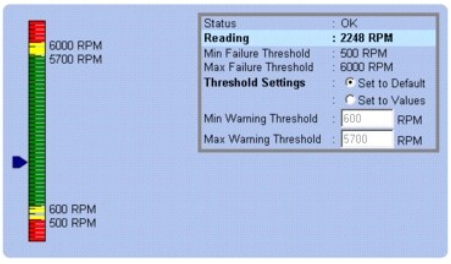
Éléments soulignés

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

Indicateurs de niveau

Les sondes de température, les sondes de ventilateur et les sondes de tension sont représentées par un indicateur de niveau. Par exemple, Figure 4-3 illustre les mesures d'une sonde de ventilateur de l'UC du système.

Figure 4-3. Indicateur de niveau



Utilisation de l'aide en ligne

Une aide en ligne contextuelle est disponible pour chaque fenêtre de la page d'accueil de Server Administrator. En cliquant sur **Aide** sur la barre de navigation globale, vous pouvez ouvrir une fenêtre d'aide indépendante contenant des informations détaillées sur la fenêtre spécifique que vous consultez. L'aide en ligne est conçue pour vous guider parmi les actions spécifiques requises pour mener à bien toutes les phases des services de Server Administrator. L'aide en ligne est disponible pour toutes les fenêtres que vous pouvez consulter, en fonction des groupes logiciels et matériels que Server Administrator découvre sur votre système et de votre niveau de privilèges d'utilisateur.

Utilisation de la page d'accueil Préférences

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

Voir Tableau 4-3 pour les options de configuration disponibles de la page d'accueil Préférences.

Tableau 4-3. Options de configuration de la page d'accueil Préférences

	.....	Paramètres généraux
	.....	Server Administrator

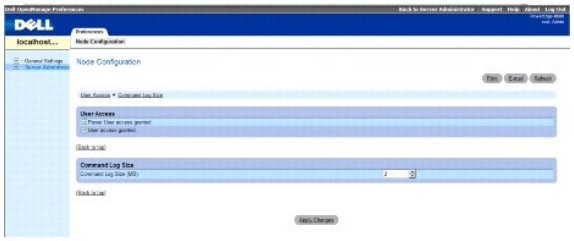
Vous pouvez afficher l'onglet **Préférences** une fois la session ouverte pour gérer un système distant. Cet onglet est également disponible lorsque vous ouvrez une session pour gérer Server Administrator Web Server ou le système local.

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

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

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

Figure 4-4. Exemple de page d'accueil Préférences



- Managed System

Préférences de Managed System

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

Cliquez sur l'objet Server Administrator pour activer ou désactiver l'accès pour les utilisateurs disposant de privilèges d'utilisateur ou d'utilisateur privilégié. Selon les privilèges de groupe de l'utilisateur, la fenêtre d'action de l'objet Server Administrator peut intégrer l'onglet **Préférences**.

Sous l'onglet Préférences, vous pouvez :

- Activer ou désactiver l'accès pour les utilisateurs ayant des privilèges d'utilisateur ou d'utilisateur privilégié.
- Configurer la taille du journal des commandes
- Configurer le protocole SNMP.

Préférences de Server Administrator Web Server

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

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

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

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

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

Cette section aborde les sujets suivants :

- Configuration des préférences utilisateur et système
- Gestion du certificat X.509

Configuration des préférences utilisateur et système

Vous définissez les préférences utilisateur et système de port sécurisé dans la page d'accueil **Préférences**.

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

Pour configurer vos préférences utilisateur, procédez comme suit :

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

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

2. Cliquez sur **Paramètres généraux**.

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

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

4. Pour changer l'apparence de la page d'accueil, sélectionnez une valeur alternative dans les champs **apparence** ou **couleurs** et cliquez sur **Appliquer les changements**.

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

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

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

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

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

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

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

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

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

   - Les champs **Nom du serveur SMTP** et **Suffixe DNS du serveur SMTP** spécifient le protocole de transfert de courrier simple (SMTP) et le suffixe du serveur de noms de domaine (DNS) de votre entreprise ou organisation. Pour que Server Administrator puisse envoyer des e-mails, vous devez taper l'adresse IP et le suffixe DNS du serveur SMTP de votre entreprise ou organisation dans les champs appropriés.

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

   - Le champ **Taille du journal des commandes** spécifie la taille de fichier maximale en Mo du fichier du journal des commandes.

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

   - Le champ **Lien de support** précise l'URL de la société qui fournit un support pour votre système géré.
   - Le champ **Délimiteur personnalisé** spécifie le caractère utilisé pour séparer les champs de données dans les fichiers créés avec le bouton **Exporter**. Le caractère **;** est le délimiteur par défaut. Les autres options sont **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **|** et **,**.
   - Le champ **Cryptage SSL** spécifie les niveaux de cryptage des sessions HTTPS sécurisées. Les niveaux de cryptage disponibles sont **Négociation automatique** et **128 bits ou plus**.

- **Négociation automatique** : permet une connexion à partir d'un navigateur avec n'importe quel niveau de cryptage. Le navigateur négocie automatiquement avec le serveur Web de Server Administrator et utilise le niveau de cryptage disponible le plus élevé pour la session. Les navigateurs hérités ayant des niveaux de cryptage plus faibles peuvent se connecter à Server Administrator.
- **128 bits ou plus** : permet des connexions à partir de navigateurs ayant un niveau de cryptage de 128 bits ou plus élevé. Une des clés de chiffrement suivantes s'appliquera à chaque session établie en fonction de votre navigateur :

SSL_RSA_WITH_RC4_128_SHA

SSL_RSA_WITH_RC4_128_MD5

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

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

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

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

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

Gestion du certificat X.509

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

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

REMARQUE : Vous devez être connecté avec des privilèges d'administrateur pour pouvoir effectuer la gestion des certificats.

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

Vous pouvez utiliser cette option pour :

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

Onglets d'action de Server Administrator Web Server

Lorsque vous ouvrez une session pour gérer Server Administrator Web Server, les onglets d'action suivants s'affichent :

- Arrêt
- Journaux
- Gestion des sessions

Contrôle de Server Administrator

Server Administrator démarre automatiquement chaque fois que vous redémarrez le système géré. Pour démarrer, arrêter ou redémarrer Server Administrator manuellement, suivez les instructions suivantes.

REMARQUE : Pour contrôler Server Administrator, vous devez avoir ouvert une session avec des privilèges d'administrateur (avoir ouvert une session en tant que root sur un système d'exploitation Red Hat® Enterprise Linux® ou SUSE® Linux Enterprise Server pris en charge).

Démarrage de Server Administrator

Systèmes d'exploitation Microsoft Windows pris en charge

Pour lancer Server Administrator sur un système qui fonctionne sous un système d'exploitation Microsoft Windows pris en charge, effectuez les étapes suivantes :

1. Ouvrez la fenêtre **Services**.
2. Cliquez-droite sur l'icône **Service de connexion de Dell Systems Management Server Administration (DSM SA)**.
3. Cliquez sur **Start** (Démarrer).

Systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge

Pour démarrer Server Administrator sur un système qui fonctionne sous un système d'exploitation Red Hat Enterprise Linux ou SUSE Linux Enterprise Server pris en charge, exécutez la commande suivante dans la ligne de commande :

```
dsm_om_connsvc start
```

Arrêt de Server Administrator

Systèmes d'exploitation Microsoft Windows pris en charge

Pour arrêter Server Administrator, effectuez les étapes suivantes :

1. Ouvrez la fenêtre **Services**.
2. Cliquez-droite sur l'icône **Service de connexion DSM SA**.
3. Cliquez sur **Arrêter**.

Systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge

Pour arrêter Server Administrator sur un système qui fonctionne sous un système d'exploitation Red Hat Enterprise Linux ou SUSE Linux Enterprise Server pris en charge, exécutez la commande suivante dans la ligne de commande :

```
dsm_om_connsvc stop
```

Redémarrage de Server Administrator

Systèmes d'exploitation Microsoft Windows pris en charge

Pour redémarrer Server Administrator, effectuez les étapes suivantes :

1. Ouvrez la fenêtre **Services**.
2. Cliquez-droite sur l'icône **Service de connexion DSM SA**.
3. Cliquez sur **Redémarrer**.

Systèmes d'exploitation Red Hat Enterprise Linux et SUSE Linux Enterprise Server pris en charge

Pour redémarrer Server Administrator sur un système qui fonctionne sous un système d'exploitation Red Hat Enterprise Linux ou SUSE Linux Enterprise Server pris en charge, exécutez la commande suivante dans la ligne de commande :

```
dsm_om_connsvc restart
```

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

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

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

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

Retour à la page du sommaire

Retour à la page du sommaire

Nouveautés de la version 6.1

Dell™ OpenManage™ Server Administrator version 6.1 Guide d'utilisation

Voici les principales caractéristiques d'OpenManage Server Administrator 6.1 :

- Prise en charge par Server Administrator des systèmes VMware® ESXi 3.5 et ESXi 4.0.
- Prise en charge des nouveaux systèmes xx1x.
- Prise en charge de trois types d'ouverture de session Server Administrator :
  - Ouverture d'une session sur le système local
  - Ouverture d'une session sur le système géré
  - Ouverture d'une session Web Server
- Prise en charge de la fonctionnalité Journal des commandes dans Server Administrator Web Server
- Prise en charge de l'affichage des options de configuration du BIOS :
  - Multitraitement principal
  - Option d'amorçage UEFI (Unified Extensible Firmware Interface)
  - Option d'état C de l'UC
  - Configuration vidéo intégrée
  - Execute Disable (Désactivation de l'exécution)
- Prise en charge d'informations sur plusieurs emplacements au sein des systèmes modulaires
- Prise en charge des composants système suivants :
  - Configuration du signalement d'attributs supplémentaires sur l'écran LCD du panneau avant (tels que le nom du système, l'adresse MAC et l'adresse IP)
  - Signalement de la présence de la carte iDRAC6 Enterprise et de la taille de stockage, le cas échéant
- Signalement de la présence de nouveaux périphériques PCI faisant partie intégrante des systèmes xx1x
  - Affichage du mode turbo de l'UC
  - Affichage des nouveaux types de mémoire (DDR3 Registered, DDR3 Unregistered)
  - Affichage des nouveaux types de logement (PCIe Gen1/2)
  - Activation/désactivation de l'architecture NUMA (Non-Uniform Memory Architecture) lors du déploiement
  - Activation de la prise en charge de l'interface à bande latérale du contrôleur de réseau sur chacun des LOM à titre individuel pour l'ensemble des LOM
  - Signalement des modes d'exploitation de la mémoire (optimiseur, en miroir, ECC avancé)
  - Configuration du délai de récupération de l'alimentation secteur
  - Configuration du port COM pour la connexion série des plateformes applicables des systèmes à partir de la version xx1x
  - Affichage des attributs de NIC physiques et des statistiques de transmission/réception
- Prise en charge améliorée du contrôle de l'alimentation :
  - Signalement des valeurs de consommation de puissance exprimées en BTU (British Thermal Unit), ainsi qu'en watt.
  - Prise en charge de la hauteur de puissance maximale et de la hauteur instantanée
  - Prise en charge du plafond de bilan de puissance pouvant être défini par l'utilisateur
  - Prise en charge du signalement de la consommation de puissance potentielle maximale et de la consommation de puissance potentielle minimale
  - Prise en charge du signalement de la puissance d'entrée nominale du bloc d'alimentation
  - Prise en charge de la fonction de génération d'alertes d'événements pour la consommation de puissance maximale
  - Prise en charge des options de profils de puissance qui peuvent optimiser les performances du système et conserver l'énergie
- Intégration d'Internet Protocol version 6 (protocole Internet version 6) :
  - Cette version prend en charge IPv6, en plus d'IPv4.
- Prise en charge supprimée de SUSE Linux Enterprise Server (Version 9).

REMARQUE : Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez la *matrice de prise en charge logicielle des systèmes Dell* qui se trouve dans le dossier **DVD_Drive\docs\readme\PEOSOM** sur le support fourni par Dell ou sur le site Web de support de Dell à l'adresse support.dell.com.

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

Retour à la page du sommaire